UNIVERSITÉ DE MONTRÉAL

INFLUENCE DES TESTS D'INTRUSION SUR L'ÉVALUATION DES RISQUES

ALEXANDRE PIEYRE

DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INFORMATIQUE)

AOÛT 2017

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

INFLUENCE DES TESTS D'INTRUSION SUR L'ÉVALUATION DES RISQUES

présenté par : PIEYRE Alexandre

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. ROBILLARD Pierre N., D. Sc., président

M. FERNANDEZ José M., Ph. D., membre et directeur de recherche

M. ROBERT Benoit, Ph. D., membre.

DÉDICACE

Je dédicace ce mémoire à mes parents, ma sœur et ma femme.

REMERCIEMENTS

Mes remerciements vont à mes partenaires scolaires et industriels dans cette aventure de création d'une méthodologie d'évaluation des risques relatifs à la sécurité de l'information.

J'aimerais donc remercier l'École Polytechnique de Montréal pour la structure dont j'ai pu bénéficier durant la période de recherche. Plus spécifiquement le Professeur José Fernandez, mon directeur de recherche. Fort de son expérience et de sa vision propre à la sécurité de l'information, il a su m'orienter et me supporter durant l'effort de recherche.

Par la suite, mes remerciements vont à mon partenaire industriel, l'entreprise OKIOK. La structure interne et les équipes m'ont permis d'orienter la méthodologie sur un modèle d'affaires concret et sur une réalité des marchés actuels en sécurité de l'information. Je tiens donc à remercier Cindy Walsh, Claude Vigeant, François Daigle et mon équipe de test d'intrusion.

Finalement, je remercie grandement mes parents, ma sœur et ma femme pour leur appui constant et indispensable.

RÉSUMÉ

La sécurité de l'information est un domaine prenant un essor considérable suite aux attaques informatiques fréquentes ayant fait l'objet d'une couverture médiatique internationale, depuis les dix dernières années. Nous sommes donc à l'ère où la protection de l'information numérique représente un enjeu capital pour les entreprises et les gouvernements. Ces acteurs sont de plus en plus sujets à la numérisation de leur processus d'affaires et des documents associés. Les attaques informatiques auxquelles ils sont exposés ont donc des impacts d'autant plus importants selon la criticité de l'information.

L'évaluation des risques informatiques est la discipline permettant d'analyser les actifs informationnels détenus par ces acteurs. Elle a pour but d'en évaluer les différents aspects de sécurité afin d'identifier les risques, les évaluer et formuler des recommandations pour les réduire. Pour cela, les méthodologies actuelles d'évaluation des risques se basent principalement sur des scénarios de menaces pouvant potentiellement se matérialiser sur l'environnement informatique d'une entreprise. Ces approches prennent pour acquis que la démarche d'analyse de risque repose principalement sur l'énumération de scénarios de menaces qui sont génériques et peu adaptés à l'environnement de l'entreprise concernée.

Nous sommes donc arrivés à nous questionner sur plusieurs aspects liés à la validité des processus d'analyse et d'évaluation des risques informatiques. Cette notion de risque informatique n'a cessé de croître durant les vingt dernières années, et ce principalement dû à la médiatisation des incidents de sécurité ainsi qu'à la prise de conscience concernant l'importance des actifs informationnels numériques, tant du côté corporatif qu'individuel. L'évaluation des risques informatiques est désormais une des préoccupations principales des entreprises soucieuses de la protection liée à leurs actifs informationnels.

L'interconnexion constante des réseaux d'information augmente considérablement la surface d'attaque permettant d'engendrer un problème de disponibilité, d'intégrité ou de confidentialité au niveau de l'information ciblée. Le constat effectué à travers l'effort de recherche ne permet pas de recenser actuellement, sur les solutions et méthodologies existantes, une méthodologie

d'évaluation des risques se basant sur des intrants concrets, empiriques et non basés sur des scénarios hypothétiques.

L'approche proposée dans ce mémoire reflète l'idée fondatrice d'une nouvelle méthodologie. Elle permet de se démarquer de l'approche par scénarios, en s'efforçant de prendre en compte les différentes sources d'informations identifiées comme tangibles pour permettre la création d'un processus de gestion des risques fiable et adapté à la réalité des entreprises. Pour cela, nous avons tiré profit de l'expérience en test d'intrusion de l'entreprise partenaire pour consolider cet intrant comme source principale dans le processus de gestion de risques.

Les tests d'intrusion sont des attaques informatisées, en temps réels, permettant de simuler l'approche qu'un attaquant utiliserait pour extraire de l'information privée sur un réseau informatique ou un système d'information, et en exploitant certaines de leurs vulnérabilités logiques. Les tests d'intrusion peuvent avoir une portée très réduite en se concentrant sur un actif ou un type d'information en particulier. Ils peuvent aussi cibler des portions de site entières.

Évaluer le risque par ce biais nous permet d'obtenir deux groupes opérationnels distincts produisant plusieurs livrables pour arriver aux fins escomptées. Le groupe en charge des tests d'intrusion s'oriente vers l'obtention d'informations précises sur la surface d'attaque des actifs informationnels de l'entreprise. Le groupe d'évaluation des risques récolte les informations sur les vecteurs d'attaque et le contexte de l'entreprise pour alimenter le modèle d'analyse, d'évaluation et de traitement des risques.

Il s'attèle par la suite à la création d'indicateurs sur la posture de risque et de traitement concernant les contrôles les plus adaptés pour éliminer les risques identifiés.

Les résultats obtenus permettent de considérer avec sérieux l'aspect méthodologique avancé à travers cette recherche. L'effet de priorisation du traitement des risques adapté au contexte de l'environnement numérique de l'entreprise a été positivement relevé et constaté par plusieurs clients lors de projets pilotes et lors de l'implantation en milieu réel. De plus la méthodologie permet de baser les contrôles de traitement sur des normes internationales en sécurité de l'information, favorisant l'ajout d'une couche de guidage et d'adaptation au contexte de l'entreprise.

Les efforts effectués dans la création de la méthodologie d'évaluation des risques informatiques permettent de répondre à un besoin particulier, celui de prioriser le traitement des risques et de réduire les imprécisions liées aux perceptions des risques, par le biais de scénarios de menace tirés des attaques perpétrées lors des tests d'intrusion. Ces imprécisions renforcent une divergence de perception entre les équipes opérationnelles et les gestionnaires responsables de la sécurité de l'information. La tendance réactive actuelle propre à l'administration des systèmes d'information implique un procédé d'évaluation des risques peu mature, peu maintenu et souvent très lourd et coûteux à mettre en place.

Les résultats obtenus lors de cette recherche permettent de prouver qu'un processus allégé et axé sur des résultats techniques de vulnérabilité informatique permettrait de complémenter l'approche par scénario et ainsi de mieux adresser les risques actuels en matière de sécurité informatique.

ABSTRACT

The security of digital information is an area of extreme importance nowadays, since the various attacks on the Internet have been the focus of international media coverage for the last ten years. We therefore are in an era where the protection of information is a key issue for businesses and governments. These actors are increasingly subject to the digitization of their business processes and related documents. The attacks they are exposed to can have severe impacts depending on the criticality of the proprietary information concerned.

Computer risk assessment is the discipline used to analyze the information assets held by these enterprises and governments. Its purpose is to evaluate the various aspects of security in order to identify risks, evaluate them, and implement recommendations to reduce them. To this end, current risk assessment methodologies are based mainly on threat scenarios that could potentially materialize on a company's digital environment. These approaches enforce that the risk analysis approach relies mainly on the enumeration of threat scenarios that are generic and not adapted to the digital environment of the company concerned.

Thus, we have come to question several aspects related to the validity of the processes of analysis and evaluation of computer risks. This notion of computer risk has kept increasing for the last twenty years, mainly due to media coverage of security incidents and to raising awareness about the importance of securing digital assets. IT security risk assessment is now one of the main concerns of companies concerned about the protection of their information assets.

The constant interconnection of information networks dramatically increases the attack surface, which can lead to a flaw in term of availability, integrity or confidentiality of targeted information.

The findings achieved through the research effort do not allow presently the identification of a methodology of risk evaluation based on concrete, empirical inputs and not based on hypothetical scenarios, as used in existing solutions and methodologies in information security risk management.

The approach proposed in this dissertation reflects the founding idea of a new methodology. This methodology differentiate itself, from the scenario approach, by endeavoring to take into account the different sources of information identified as tangible to enable the creation of a reliable risk management process adapted to the reality of companies. In order to obtain this type of information on the security posture, we have taken advantage of the intrusion test experience of a partner company. This is aimed at consolidating intrusion testing input as a main source in the risk management process.

Intrusion tests are computerized attacks, in real time, to simulate the approach an attacker would use to extract private information on a computer network or an information system, exploiting some of their logical vulnerabilities. Intrusion testing can be very limited in scope by focusing on a specific asset or type of information. They can also target portions of entire sites.

Evaluating the risk in this way drives us to distinct two operational groups producing several deliverables to arrive at the intended purpose. The group in charge of the intrusion tests is oriented towards obtaining precise information on the attack surface of the company's information assets. The risk assessment group collects information on the vectors of attack and the context of the company to feed the model of analysis, evaluation and treatment of risks.

The methodology then proceeds to the creation of indicators on the posture of risk and treatment regarding the most appropriate controls to eliminate the identified risks.

The results obtained make it possible to consider with seriousness the methodological aspect advanced through this research. The effect of prioritizing the risk treatment adapted to the context of the company's digital environment was positively noted and observed by several clients during pilot projects and during the implementation in real environment. Moreover, the methodology makes it possible to base the processing controls on international standards in information security, favoring the addition of a layer of guidance and adaptation to the context of the company. Efforts to create the IT Risk Assessment methodology address a particular need to prioritize risk treatment and reduce inaccuracies in risk perceptions. Those errors and disparities in security vision and mitigation prioritization currently persist between the operational teams and the managers responsible for information security, in an enterprise.

The current reactive trend in the markets and concrete observations implies a system of risk assessment that is not very mature, little maintained and often very cumbersome and costly to put in place.

The results obtained from this research demonstrate that a streamlined process - focused on technical results of systems and computers vulnerability - would better address current security risk evaluation.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

La liste des sigles et abréviations présente, dans l'ordre alphabétique, les sigles et abréviations utilisés dans le mémoire ainsi que leur signification :

ACI Actif Informationnel

Un ACI peut être caractérisé comme n'importe quel support logique ou physique stockant de l'information numérique de manière temporaire ou définitive.

A/CA Avec Contrôle Actuel

Prenant en compte la posture de sécurité et les scores de risque avec les contrôles actuels et avant traitement.

A/CR Avec Contrôle Recommandé

Prenant en compte la posture de sécurité et les scores de risque avec les contrôles recommandés et après traitement.

AO Apprentissage Organisationnel

Stratégie d'amélioration continue pour l'apprentissage organisationnel.

ATT Attaquant

Individu ou groupe revendiquant différentes motivations et susceptible(s) d'exploiter une ou plusieurs vulnérabilité(s) dans le but d'avoir accès à un ou plusieurs actif(s) informationnel(s).

BDOV Base de Données Orientée Vulnérabilité

Base de classification des vulnérabilités selon le Domaine de Test et le mandat client. Chaque BDOV devrait être unique puisqu'elle reflète une analyse d'un EC spécifique.

CAF Catégorie d'Affaires

Permet de répertorier et regrouper les entreprises et leurs actifs informationnels selon leur secteur d'activité. Finance, Assurance, Développement logiciel, etc.

CASES Cyberworld Awareness and Security Enhancement Services

CID Confidentialité, Intégrité, Disponibilité

Pilier propre à la sécurité de l'information composé de trois principes clés : Confidentialité, Intégrité et Disponibilité.

CVSS *Common Vulnerability Scoring System*

Standard international de quantification de la sévérité d'une vulnérabilité.

DOT Domaine de Test

Le domaine qualifie un ensemble des tests et vulnérabilités propres à un environnement client. Par exemple, lors de la mise à l'épreuve d'une plateforme applicative, le domaine de test sera « Tests d'application web » . Plusieurs domaines peuvent être nécessaires à la bonne conduite du processus de test sur un environnement client. On parlera donc de plusieurs domaines de test dans le mandat concerné.

DMZ Zone démilitarisée

Zone logique de séparation entre un réseau interne d'entreprise et internet (réseau externe).

EC Environnement Client

Portée du mandat de test d'intrusion. La portée représente l'environnement numérique sur lequel seront effectués les tests d'intrusions.

EGR Équipe de Gestion des risques

Équipe comprenant les MEGR et le REGR

ETI Équipe de Tests d'Intrusion

Équipe comprenant les METI et le RETI

EV Ensemble de vulnérabilités

Groupe de vulnérabilités pouvant se rattacher à une catégorie de contrôle

FA Facteur d'affaires

Sert à déterminer les impacts financiers.

FAM Facteur d'Agent de Menace

Sert à estimer précisément, grâce aux tests d'intrusion, les groupes d'attaquants susceptibles de mener des attaques avec succès.

FIT Facteur d'impact technique

Sert à déterminer les impacts sur l'infrastructure supportant les données.

FV Facteur de Vulnérabilité

Sert à déterminer les caractéristiques et la quantification des aspects propres aux failles

GIPS Gestion des Indicateurs de Posture de Sécurité

Ensemble des indicateurs de posture de sécurité. Composé de la partie statistique des BDOV et de l'indice de maturité.

GPC Gestionnaire Projet Client

Désigne le gestionnaire de projet, compte du coté client. Ce dernier interagit de manière régulière avec l'IPM et les METI.

GPI Gestionnaire de Projet Interne

Désigne le gestionnaire de projet, compte du côté client. Ce dernier interagit de manière régulière avec l'IPM et les METI.

IDR Indice de Détection et de Réponse

Les indicateurs de détection et de réponse permettent aux membres de l'équipe de tests d'intrusion de mieux apprécier les réactions du client lors des tests. Il est à noter que cette étape est facultative, car certains clients ne seront pas enclins à divulguer leur capacité de réponse si cela n'a pas été précisé dans les règles d'engagement.

IA Intelligence artificielle

IDE Indice de découverte

Niveau de difficulté nécessaire pour découvrir la vulnérabilité.

IEP Indice d'exploitation

Niveau de difficulté nécessaire pour exploiter la vulnérabilité.

INC Indice de niveau de compétence

Niveau de compétence indique les qualifications de l'agent de menace.

IMO Indice de motivation

Niveau de valeur des données pour l'attaquant.

IOP Indice d'opportunité

L'indice d'opportunité concerne les vecteurs d'accès et les ressources nécessaires pour exploiter la vulnérabilité.

IPA Indice de population d'agent

Caractéristique du groupe représentant l'agent de menace.

ITREM *Intrusion Testing for Risk Evaluation and Management*

Processus méthodologique d'évaluation des risques basé sur les résultats des tests d'intrusion.

METI Membre de l'Équipe de Tests d'Intrusion

Les membres sont spécialisés dans l'évaluation de sécurité des environnements en procédant selon un processus d'intrusion progressif permettant de reporter les vulnérabilités à chaque étape. Ils sont responsables de l'application du processus d'identification des risques.

MEGR Membre de l'Équipe d'évaluation des risques

Les membres sont spécialisés dans l'évaluation des risques technologiques et dans la gouvernance propre à la sécurité des systèmes d'information. Ils sont responsables de l'application du processus d'appréciation et d'évaluation des risques.

PAC Processus d'Appréciation du Contexte

Détermination du contexte organisationnel et environnemental permettant de mieux cerner les besoins et attentes du client.

PAMC Processus d'Amélioration Continu

Chaine de contrôle dynamique permettant de reconduire le processus de tests d'intrusion sur le même EC pour effectuer une validation de l'étape de traitement. PAMC peut aussi conduire au test d'un autre environnent pour élargir l'évaluation des risques.

PGR Processus d'évaluation des risques

Processus de gestion continue prenant en intrant les ensembles de vulnérabilités et permettant le traitement des risques relatifs. Désigne la partie propre à ITREM et comportant la méthodologie nécessaire pour adresser, classifier, évaluer et traiter les risques d'un EC.

PTES *Penetration Testing Execution Standard*

Standard international de référence aux étapes de test d'intrusion.

PTI Processus de Test d'Intrusion

Organisation complète des tests d'intrusion, de la définition propre à la portée jusqu'à la remise du rapport.

RDV Registre dédié aux vulnérabilités

Structure de dossier contenant toutes les BDOV relatives à une catégorie d'affaires.

REGR Responsable de l'Équipe d'évaluation des risques

Responsable de la coordination de l'EGR et du suivi des mandats clients propres à l'évaluation des risques. Il est lui-même un MEGR.

RETI Responsable de l'Équipe des Test d'Intrusion

Responsable de la coordination de l'ETI et du suivi des mandats clients concernant les tests d'intrusion. Il est lui-même un METI.

RT Référence de Test

Identifiant unique permettant de faire une référence rapide au test correspondant

RSSI Responsable de la Sécurité des Systèmes d'Information

Responsable de la gestion de la sécurité informatique au sein de l'entreprise, y compris l'établissement d'une politique de sécurité définissant les objectifs de sécurité concernant les biens informatiques à protéger, en accord avec les objectifs d'affaire de l'entreprise tels que déterminés par la haute direction.

SDT Sous-domaine de test

Les sous-domaines sont les différentes parties propres à un domaine. Par exemple dans le TD propre aux applications web, un sous-domaine de test pourrait être 'Information Gathering'. Ils regroupent les unités de test.

SMSI Système de management de la sécurité de l'information

Ensemble de règles de gouvernance permettant d'assurer une gestion cyclique de la sécurité des actifs informationnels.

UT Unité de Test

Les unités de test désignent les tests pouvant être effectués sur l'infrastructure de données cible. Ils sont détaillés dans un onglet personnalisé donnant des informations sur la nature du test, ses impacts, sa portée, et les moyens permettant de conduire ces tests.

VANSS Vulnerability Analysis Scoring System

Méthodologie d'analyse quantitative de vulnérabilité, complémentaire à ITREM.

LISTE DES ANNEXES

CHAPITRE 1 ÉVALUATION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

1.1 Étude du problème

Dépendamment de l'entreprise, de la nature de ses affaires, du budget alloué aux technologies de l'information, des normes utilisées, des équipements concernés et des plateformes applicatives, il est souvent très difficile de concevoir, d'implanter et de soutenir un écosystème de gestion de la sécurité informatique qui évolue en accord avec les besoins de l'entreprise à travers le temps. Cette observation est due à une multiplication des menaces informatiques relatives aux plateformes technologiques utilisées en entreprises et une évolution constante de ces plateformes elles-mêmes, qui sont en constante évolution et qui sont d'une complexité et diversité déjà difficile à gérer. La conséquence se traduit par une tendance marquée venant souligner la difficulté de gérer la totalité de la sécurité informatique sur des infrastructures de données numériques.

La pierre angulaire de la gestion de la sécurité informatique de ces systèmes est le processus d'évaluation des risques informatiques. Ce processus a pour objectifs :

1) D'identifier les menaces contre les systèmes informatiques
2) De les prioriser en termes de risque
3) D'évaluer la réduction du risque engendré par l'introduction de différentes contre-mesures afin de choisir les plus efficaces

Pour l'étape d'identification des menaces, les approches traditionnelles d'identification par scénario sont désormais désuètes lorsqu'appliquées en sécurité informatique. Une approche par scénario aura tendance à se baser sur un scénario d'attaque bien défini avec un acteur abstrait exploitant une vulnérabilité. Le scénario est ensuite évalué en termes qualitatifs ou quantitatifs, et sur l'impact potentiel envers l'entreprise en cas de réalisation. Une fois le scénario évalué, sélectionné, et priorisé, il est possible d'y appliquer des contre-mesures et contrôles venant réduire le risque relatif au scénario, en éliminant la vulnérabilité.

Cependant, cette approche est limitative, car un environnement numérique d'entreprise comporte des centaines de scénarios d'attaques potentielles affectant la sécurité. Cela demande donc une gestion très volumineuse et peu souple des différents scénarios, et rend leur évaluation arbitraire.

Il est donc extrêmement fastidieux de prioriser les bonnes mesures de protection lorsque des centaines de scénarios sont disponibles.

La majorité des approches de gestion et évaluation des risques informatiques appliquées en entreprises sont encore basées sur des approches par scénarios. Par exemple, EBIOS [1] et ISO 31000 [2] sont toutes des méthodologies se définissant à travers des évaluations quantitatives et qualitatives de risques pour certains scénarios prédéfinis. L'évaluation des scénarios est souvent influencée par la perception de l'individu ou du groupe d'individus responsable de l'évaluation. Ceci constitue un biais de précision commun à toute méthodologie d'appréciation des risques.

Aucune méthodologie d'évaluation des risques ne permet actuellement d'établir des modèles précis sur les menaces et les potentialités relatives. Suite à de multiples questionnements sur l'évaluation des risques, et aux limitations relatives en entreprises constatées lors de différentes missions de consultation dans l'industrie, nous nous sommes intéressés à la création d'une méthodologie d'évaluation des risques informatiques qui puisse adresser certaines de ces lacunes. Les limitations relatives au manque de précision des indicateurs sur l'exposition des actifs informationnels et les menaces relatives nous permettent de poser les bases d'un questionnement sur la pertinence de considérer une approche quantitative novatrice.

Cette approche serait une partie intégrante d'une évaluation dynamique des risques, basée sur certains intrants dont :

- Les résultats de tests d'intrusion sur les systèmes informatiques
- Les observations des sondes et capteurs de surveillance déployés sur les réseaux informatiques
- Les résultats d'analyses de vulnérabilités sur les logiciels installés
- Les résultats d'analyses d'attaques informatiques passées
- Les tendances actuelles dans le domaine de la criminalité informatique

La qualité des paramètres (intrants) alimentant une telle méthodologie doit être d'une fiabilité accrue pour fournir des résultats plus précis.

Un test d'intrusion n'est autre qu'un ensemble de techniques et de tests permettant de reproduire les attaques informatiques perpétuées par des intervenants internes et/ou externes et atteignant la confidentialité, l'intégrité et la disponibilité d'un système d'information. Les tests d'intrusion sont classés majoritairement en 4 domaines : tests d'intrusion **réseau**, **applicatifs**, **mobiles** et **physiques** [3]. Ils permettent d'avoir une meilleure appréciation sur les mesures de sécurité déjà en place et donnent des indicateurs précieux sur de futures étapes à conduire pour s'orienter vers une sécurité optimale. Le but des tests consiste généralement à simuler l'attaque d'un acteur mal intentionné voulant accéder à certaines données.

Étant donné que la conduite de tests d'intrusions nécessite un niveau de connaissance et une expertise technique élevés, ces tests sont souvent réalisés par des firmes spécialisées pour le compte des entreprises qui opèrent les systèmes informatiques visés. Ainsi, ces firmes produisent pour leurs clients de longs rapports recensant les vulnérabilités propres à leur environnement (EC). L'environnement client (EC) désigne ici l'environnement numérique sur lequel les tests ont été conduits. Cependant, l'utilité de ces rapports pour le client est limitée, étant donné qu'il n'est pas possible de déterminer un niveau de risque uniquement basé sur les vulnérabilités trouvées et détaillées dans ces rapports.

De ce fait, nous voulons déterminer s'il est possible d'établir un processus clair permettant de mettre à profit les résultats de tests d'intrusion à travers une méthodologie d'évaluation des risques, afin de maximiser leur utilité dans la prise de décision dans la gestion de la sécurité informatique. Ce processus permettra de se positionner en qu'intrant complémentaire aux approches traditionnelles de gestion des risques, car il sera basé sur des intrants tangibles et non sur une base hypothétique. Les tests d'intrusion forcent l'obtention de ces indicateurs tangibles, relatifs à l'exposition et à la criticité des données.

Un des buts précis de cette recherche scientifique sera donc la création d'un modèle d'évaluation des risques, alimenté par les résultats de tests d'intrusion dans le but de renouveler un modèle décisionnel désuet se basant sur des scénarios de menaces génériques peu adaptés au contexte d'entreprise, étant donné leur grande diversité.

1.2 Objectif et questions de recherche

L'objectif de recherche de nos travaux est le suivant :

« *Élaboration et évaluation d'une méthodologie d'évaluation des risques se basant sur les résultats de tests d'intrusions, qui puisse offrir une meilleure prise de décision en gestion de la sécurité informatique par rapport aux méthodes existantes* »

Cet objectif découle partiellement du constat fait à travers l'étude des tendances et des guides méthodologiques actuellement disponibles dans le domaine de l'évaluation des risques appliquée à la sécurité informatique. Nous considérons que les processus et livrables découlant de cette recherche sont des éléments complémentaires permettant de contribuer à une base porteuse et innovante résultant en l'élaboration de la méthodologie que nous proposons. Cette méthodologie que nous avons baptisée *Intrusion Testing for Risk Evaluation and Management* (ITREM) représente donc le fruit de plusieurs questionnements sur le domaine de l'architecture de services de sécurité adaptés aux besoins d'entreprises, en matière de quantification, priorisation et traitement des risques.

Afin de pouvoir vérifier et mesurer le progrès dans l'accomplissement de cet objectif de recherche, nous poursuivrons le cheminement de ce chapitre en discutant plus en détail le problème que nous avons posé afin d'identifier et établir le bien-fondé des sous-objectifs et questions de recherches que nous nous sommes fixés dans ce travail.

Dans la pratique actuelle, les tests d'intrusion sont largement utilisés par les grandes et moyennes entreprises pour pouvoir répertorier automatiquement les vulnérabilités existantes sur leurs systèmes d'information. Comme le souligne très bien Jones [4], dans son chapitre accordé aux outils d'audit et de détection de vulnérabilités, la tendance actuelle sur le marché de la détection des vulnérabilités est tellement avancée que plusieurs manufacturiers logiciels se démarquent en multipliant les suites automatisées de découverte de failles. Nessus®, Nexpose, Core Impact [5] sont tous des exemples de logiciels spécialisés permettant d'obtenir une multitude de failles provenant du code, de la configuration, des mises à jour, etc. Le marché est très mature en ce qui a trait à ce genre d'identification. De plus, il existe déjà des bases de données de vulnérabilités qui

sont utilisées pour recenser une partie des attaques disponibles dans notre éventail de tests d'intrusion. En conséquence, on s'attend à ce qu'un test d'intrusion puisse fournir plus de valeur ajoutée qu'une simple identification logique des services vulnérables.

À l'origine l'objectif voulu des tests d'intrusion « classiques » était d'évaluer le risque informatique de façon globale en se mettant volontairement dans un scénario d'attaque, dans lequel une équipe de test joue le rôle de l'attaquant et essaie de pénétrer le périmètre de sécurité des systèmes afin d'accomplir un objectif malveillant simulé. Le succès et la facilité relative de cette équipe de test d'intrusion à accomplir ses objectifs constituent donc un indicateur indirect de la potentialité que ces attaques soient réalisées par un authentique adversaire malveillant. Or cet indicateur est très imparfait, car il est difficile pour l'équipe de parcourir tous les scénarios d'attaque possibles, d'une part, et de l'autre il ne tient pas compte de l'importance relative des biens informatiques pouvant avoir été ciblés par l'équipe de test d'intrusion. En d'autres mots, les résultats de test d'intrusion dans ce contexte ne servent que d'indicateur de potentialité, et non pas d'impact. En fait, ce qui semble évident et intuitif est que l'impact d'un scénario dépendra de l'importance du bien informatique ciblé par cette attaque, ou en d'autres mots du *contexte* dans lequel ce scénario d'attaque aura lieu, qu'il soit un contexte réseau (p.ex. segment de réseau contenant les serveurs), un contexte applicatif (p.ex. les applications reliées aux transactions financières) ou un contexte usager (p.ex. les données stratégiques compétitives reliées à la haute direction). Cette réflexion nous amène donc à une première question de recherche :

1. *Comment prendre en compte les informations de contexte des systèmes informatiques dans le processus d'évaluation des risques*

De plus, malgré que les vulnérabilités identifiées par les outils de tests d'intrusion mentionnés ci-haut correspondent en grande majorité à celles décrites dans des bases de données de vulnérabilités, les extrants des outils utilisés génèrent des rapports de format variable et contenant des informations techniques qui sont difficilement interprétables et difficilement utilisables directement dans l'évaluation des risques. Ainsi, afin de pouvoir utiliser les résultats des tests d'intrusion dans un processus intégré d'évaluation des risques, nous devons adresser la question suivante :

2. *Comment adapter, standardiser et même optimiser le processus de test d'intrusion afin de pouvoir utiliser ses extrants à des fins d'évaluation des risques ?*

Nous postulons donc que si les informations sur les vulnérabilités identifiées dans les résultats des tests d'intrusion peuvent être transformées de façon à les rendre plus facilement interprétables et peuvent aussi être reliées à un contexte informatique où elles sont présentes, il est alors théoriquement possible pour l'analyste de sécurité d'évaluer le risque (autant en potentialité qu'en impact) relié à chacun des scénarios pouvant exploiter ces vulnérabilités. Cependant, le nombre de vulnérabilités identifiées lors de tests d'intrusion typiques reste très élevé, se situant souvent dans les centaines voire des milliers d'incidences rapportées. Ceci rend donc peu viable notre proposition à moins que nous puissions automatiser partiellement ou totalement le processus de classification des vulnérabilités en termes de risque, un processus imbriqué lui-même dans le processus d'évaluation et gestion des risques informatiques, qui lui tient compte entre autres de la réduction du risque introduit par les contrôles de sécurité. C'est à cet effet que nous proposons d'utiliser des approches d'apprentissage machine afin d'assister l'analyste de sécurité dans cette tâche, ce qui adresse la question de recherche suivante :

3. *Comment automatiser le processus de classification des vulnérabilités ?*

Finalement, toute proposition théorique de méthodologie d'évaluation de risques telle que celle que nous proposons doit pouvoir démontrer sa réelle valeur dans la pratique professionnelle. Le succès d'une telle méthodologie et sa viabilité dans la pratique professionnelle dépendent d'une part de sa capacité à aider à prendre des décisions judicieuses - et donc dans sa précision à prédire les risques informatiques -, et de l'autre de sa viabilité en termes de difficulté d'utilisation, coût, etc. À cette fin, nous avons eu la chance d'utiliser la méthodologie proposée en pratique professionnelle avec un client réel ce qui nous a permis d'adresser partiellement la question de recherche suivante :

4. *Est-ce que l'utilisation des résultats de tests d'intrusion permettrait dans un contexte d'utilisation réelle d'augmenter de façon viable le niveau de précision lors de l'étape d'identification, d'analyse, d'évaluation et de décision sur les risques spécifiques à la*

sécurité de l'information, tout en n'imposant pas un coût et un effort supplémentaire démesurés ?

1.3 Cheminement méthodologique

L'exercice de production de la méthodologie est venu d'une idée prenant comme intrants les observations effectuées dans des entreprises de différents secteurs, en ce qui a trait à la gestion de la sécurité de leurs actifs. Comment harmoniser et standardiser les approches de gestion des vulnérabilités à travers une méthodologie d'évaluation des risques en utilisant une base moins subjective que celle des méthodes existantes ?

Deux acteurs principaux m'ont permis de réaliser ce projet à terme, à travers une bourse de recherche MITACS. Mon partenaire académique, l'École Polytechnique de Montréal et plus particulièrement mon directeur de recherche, José Fernandez, m'a orienté de façon à dresser les processus majeurs permettant d'articuler la méthodologie.

Le partenaire industriel, Okiok, entreprise spécialisée en sécurité informatique, a manifesté un intérêt pour débuter une collaboration basée sur le développement d'un modèle de référence en matière de tests d'intrusion. Ces derniers seraient utilisés pour alimenter une méthodologie d'évaluation de risque, reflétant la posture de sécurité d'un environnement caractérisé par des actifs informationnels variés et nécessitant une sécurité accrue.

La première partie de ce processus méthodologique est donc la reprise du processus de tests d'intrusion (PTI) de façon à le décomposer et à l'optimiser pour obtenir des résultats standardisés et interprétables par le mécanisme de traitement postérieur.

De ce fait, les résultats, sous forme standardisée, peuvent être appréciés plus précisément à travers un processus venant apporter une dimension extrêmement importante en gestion des risques. En effet, l'appréciation du contexte d'affaires permet de cerner quels sont les actifs les plus à risque pour l'entreprise. Cette étape vient aussi considérer les aspects de maturité ainsi que les normes, standards, et obligations légales de l'entreprise concernant la gestion de la sécurité informatique. Le processus d'appréciation du contexte (PAC) permet de reprendre et conditionner les

vulnérabilités identifiées dans le processus de tests d'intrusion, de façon à les standardiser et attribuer certaines pondérations utilisées dans le cadre du processus d'évaluation des risques (PER).

Dans cette optique, le processus d'évaluation des risques permet, à travers un moteur d'analyse quantitative, d'obtenir des scores de risque précis qui permettront une classification en fonction des actifs impactés et des types de vulnérabilités répertoriées. Ce processus permet de dresser la liste des risques évalués, leurs impacts sur l'entreprise, leurs potentialités et leur appartenance relative aux ensembles de vulnérabilités (EV). Cette classification par ensembles de vulnérabilités est conçue de façon à favoriser, lors de l'étape d'évaluation de contre-mesures, une réduction applicable à plusieurs risques de la même catégorie. Cela conforte la dimension d'efficacité des traitements appliqués et donc de réduction des risques résiduels.

Ce processus d'évaluation des risques constitue le cœur de cette méthodologie. Il doit donc être optimisé pour répondre à une forme de continuité à travers un processus cyclique. L'idée à travers cette continuité est d'établir un processus global et cyclique venant évaluer non seulement les risques de l'environnement ciblé, mais aussi les progrès propres aux traitements des risques évalués et priorisés.

Pour répondre à cette continuité du processus méthodologique, nous avons créé un processus s'apparentant plus à de l'apprentissage organisationnel et qui permet d'assurer un suivi régulier des progrès en gestion des risques, découlant du processus d'évaluation des risques.

1.4 Vue globale du mémoire

Le reste de ce mémoire est constitué des parties suivantes. Le chapitre 2 permet de mieux comprendre le contexte actuel en termes de gestion des risques. Il introduit l'état de l'art en gestion de la sécurité informatique, notamment la difficulté de planifier un programme de sécurité adapté à l'environnement numérique. Il décrit également la pratique en termes de tests d'intrusion et de leur utilisation peu efficace dans la gestion des risques. Pour mener à bien l'étude de la problématique, un effort de recherche documentaire a été effectué et permet de distinguer 5 phases

distinctes autour desquelles graviteront les différentes parties de la revue de littérature. Parmi ces phases, nous comptons :

1) La tendance propre aux tests d'intrusion
2) L'identification des évènements affectant la sécurité de l'information
3) Les méthodes quantitatives d'analyse des risques
4) L'innovation dans le domaine de l'évaluation des risques ainsi que de l'investissement
5) La prise de décision découlant de l'exercice de gestion des risques

Ce chapitre nous permettra de conditionner et d'appuyer le raisonnement développé lors du chapitre 3.

À cet effet, le chapitre 3 décrit les grandes lignes de la méthodologie ainsi que l'ontologie de l'évaluation des risques propre à ITREM. Nous y découvrirons comment s'imbriquent les 4 processus majeurs sur lesquels est basé l'effort méthodologique.

Le chapitre 4, quant à lui, sera dédié à apporter tout le détail nécessaire pour comprendre les calculs de risque. Il fera mention des mesures, indices et facteurs permettant l'évaluation quantitative des risques relatifs aux vulnérabilités identifiées lors de l'exercice de tests d'intrusion.

Plus particulièrement, nous dédions un chapitre séparé à nos efforts d'automatisation du processus de classification de vulnérabilités dans le contexte d'ITREM, afin d'alléger la tâche des membres de l'équipe de gestion des risques. Au chapitre 5 nous décrivons les techniques d'intelligence artificielle en apprentissage machine que nous avons utilisées pour construire un système de classification qui permet de classifier automatiquement les vulnérabilités découvertes lors de tests d'intrusion en termes de priorité de traitement. Nous décrivons les résultats obtenus lors de l'évaluation de ce mécanisme de classification automatisé.

Pour appuyer notre raisonnement et le développement de notre méthodologie, nous introduirons les étapes d'application d'ITREM en entreprise lors de l'analyse d'une étude de cas. Cela sera effectué lors du chapitre 6, et permettra de valider la méthodologie et ses processus sous-jacents en milieu réel.

Finalement, le chapitre 7 nous permettra de revenir sur les questions de recherches, les différentes parties du mémoire, ainsi que sur les travaux futurs.

CHAPITRE 2 GESTION DES RISQUES INFORMATIQUES

2.1 État de l'insécurité informationnelle

Cette sous-partie du chapitre 2 est nécessaire pour comprendre et cerner les prémisses de cet effort de recherche. Elle permettra, dans la continuité de ce chapitre, d'exposer les solutions actuelles en matière d'évaluation des risques et en ce qui a trait à l'orientation des responsables et des différents investissements en matière de sécurité de l'information. De plus, une revue et une analyse critique de certains articles de recherche, en rapport avec les tests d'intrusion et les mécanismes d'évaluation des risques, seront effectuées afin de mieux comprendre l'orientation du travail actuel en termes d'innovation et de solutions.

Les organisations ont besoin d'outils pratiques, précis, et permettant d'obtenir des indicateurs concrets et une analyse comparative interne de la sécurité informatique avec des standards reconnus, afin de planifier efficacement leur stratégie et le plan directeur de la sécurité informationnelle. La tendance actuelle en matière de gestion de la sécurité de l'information sur la scène mondiale consiste en des entreprises de plus en plus conscientes du danger lié à l'exposition de leurs actifs. Cependant, les budgets alloués aux départements des technologies de l'information, et plus précisément au domaine de la sécurité et de la protection des actifs informationnels, restent peu adaptés et reflètent malheureusement une politique d'investissement austère. Les deux facettes principales de cette réalité sont simples [6] :

- La formation et la sensibilisation des hauts dirigeants à l'importance des actifs informationnels de l'entreprise et aux contrôles permettant de les protéger sont peu développées
- La sécurité de l'information est un domaine sans profitabilité (financièrement parlant) et se caractérise par un investissement voué à réduire la posture de risque

Il est donc commun de constater un manque d'engouement chez certains hauts dirigeants en ce qui a trait à la sécurité de leurs actifs numériques. Ce manque d'information concernant les orientations et le positionnement en matière de sécurité pousse les dirigeants et responsables des systèmes

d'information à établir des stratégies réactives positionnant l'entreprise en porte à faux avec ses objectifs de sécurité.

De plus, les membres de la direction se soucient peu de savoir réellement quels sont les moyens techniques permettant d'assurer la protection de l'entreprise et de ses services informatisés. Ce qui importe le plus, c'est d'être capable de saisir et d'évaluer précisément quels sont les coûts associés aux impacts sur les actifs informationnels. De façon à déterminer le budget nécessaire aux opérations optimales en termes de sécurité, il est nécessaire de répondre à ces questions :

- Quels sont les actifs les plus à risque dans l'entreprise ?
- Quelle est leur posture de sécurité actuelle ?
- Quels seraient les impacts et coûts relatifs à une attaque ?
- Quelles sont les solutions les plus effectives ?

Ces questionnements paraissent essentiels pour tout acteur familier avec les principes de sécurité de l'information. Cependant, les réponses demandent un effort d'analyse et de recherche requérant un appui constant de la haute direction ainsi qu'une communication bilatérale entre plusieurs départements clés de l'entreprise. La raison principale réside dans le fait que le Responsable de la Sécurité des Systèmes d'Information (RSSI) se doit d'agir à différents niveaux pour assurer la sécurité des actifs tout en respectant l'alignement avec les objectifs d'affaire et les contraintes légales. Le RSSI a pour but, dans ses tâches principales, d'assurer un suivi constant ainsi qu'une continuité entre les décisions de la haute direction et les répercutions qu'elles impliquent au niveau de la priorisation sur les contrôles techniques. Les contrôles, propres à des référentiels comme le NIST SP800-53 (émis par le *National Institute of Science and Technology*) sont des prérequis et constituent des lignes directrices permettant d'orienter le gestionnaire de la sécurité de façon à couvrir tous les domaines propres à la sécurisation des actifs. À cet effet, les contrôles permettent au RSSI de mettre en place des contre-mesures technologiques, procédurales, et légales pour diminuer les impacts relatifs aux données dont il est le garant en matière de sécurité.

2.2 Tests d'intrusion et identification de vulnérabilité

Le guide de référence, à l'échelle d'internet, concernant les tests d'intrusion est celui du *Penetration Testing Execution Standard* (PTES) [7]. Ce dernier, considéré comme un standard de test de pénétration, est composé de sept sections principales. Pour information, un test de pénétration est aussi un test d'intrusion.

Celles-ci couvrent tout ce qui concerne un test d'intrusion - de la communication initiale au raisonnement derrière un *pentest* (synonyme), à travers la collecte de renseignements et la modélisation des menaces ainsi que les phases où les testeurs travaillent en arrière-plan afin d'obtenir une meilleure compréhension de l'organisation testée. Ce processus combine donc la recherche de vulnérabilité à l'expertise des chercheurs ainsi qu'à la compréhension du contexte de l'environnement testé de façon à bénéficier d'une valeur ajoutée maximale.

Cependant, le guide se concentre à haut niveau sur le processus complet de test de pénétration ainsi que sur les différents types de vulnérabilités que l'on peut identifier en fonction des systèmes d'exploitation. Quand bien même ce dernier reste complet, peu de détails techniques sont actuellement disponibles.

Contrairement à PTES, un des guides valorisants en termes d'aide à la compréhension en recherche de vulnérabilités et d'attaques est celui émis par David Maynor, « Metasploit Toolkit » [8].

Ce dernier est un excellent livre pour comprendre les principes d'exploitation à travers une plateforme facilitant le processus global d'intrusion dans un système d'information, mais les outils ne sont pas forcément à jour avec les dernières trouvailles en termes de vulnérabilités. Cependant, Metasploit reste un pilier fondateur de la sécurité offensive. Il permet, en plus d'obtenir une interface intuitive pour la gestion des attaques, d'implanter une plateforme de création personnalisée d'exploits. Cela propulse l'outil et l'utilisateur dans une dimension plus flexible et certainement plus soutenue techniquement comparativement à celle des plateformes complètement automatisées se limitant à un sous-ensemble d'exploits connus et bien souvent obsolètes de par les contre-mesures et mise à jour de sécurité implémentées.

Un des aspects manquants dans Metasploit est la recherche automatisée de vulnérabilités sur les plateformes applicatives de type web.

De plus, une lacune significative en ce qui concerne les tests de pénétration web est à souligner. A cet effet, un des efforts de recherche a été axé vers l'assimilation des connaissances disponibles à travers l'OWASP [9], la base de référence en termes d'attaques et de détection de vulnérabilités web.

OWASP est une communauté ouverte dédiée aux organisations, permettant de concevoir, développer, acquérir, exploiter et maintenir des applications sécuritaires et durables. Tous les outils, documents, et forums de l'OWASP sont gratuits et ouverts à toute personne intéressée à l'amélioration de la sécurité applicative et web.

En dépit du fait que les deux bases citées ci-dessus sont d'excellentes ressources pouvant être utilisées dans le but d'élaborer un éventail de services et prestations de tests d'intrusion, il est nécessaire de les coupler avec un répertoire de CVE. Les CVE (Common Vulnerability Exposure), cataloguent chaque vulnérabilité publiée publiquement, et sont toutes regroupées par manufacturier d'équipement et de logiciel dans la NVD (National Vulnerability Database).

La majorité des entreprises offrant des services de tests d'intrusion basent leurs approche sur les trois ressources énoncées plus haut. La différentiation dans la qualité et la fiabilité de la prestation de service se traduit donc sur l'expertise des ressources effectuant les tests d'intrusion ainsi que sur la forme du processus utilisé, de la recherche des vulnérabilités jusqu'à la présentation de ces dernières.

De ce fait, ce raisonnement basé sur la formation et la capacité des ressources à trouver les vulnérabilités pourrait potentiellement introduire une marge d'erreur quant à la détection systématique de vulnérabilité pouvant mener à une atteinte aux principes premiers de la sécurité de l'information.

Ce constat est aussi une cause de la pratique des tests de sécurité, prenant en compte le fait que cette dernière soit une niche dans le secteur de la sécurité de l'information. Les acteurs principaux

ainsi que les firmes de sécurité, concurrentes, sont soucieux de garder leur mode opérationnel ainsi que leurs outils et techniques spécifiques.

Pour réduire de manière résiduelle cette marge d'erreur, il est nécessaire de construire une plateforme permettant de servir de référence technique aux différentes ressources. Aucune référence actuelle, autre que celles citées plus haut et se concentrant sur un domaine particulier, n'a encore de base conséquente renfermant plusieurs centaines de techniques d'exploitation.

Aucune méthodologie ne propose actuellement des intrants techniques tels que les résultats de tests d'intrusion, pour servir de base à une approche d'évaluation des risques. Les seuls points de similarité potentiellement disponibles dans les solutions professionnelles sont les indicateurs de risques développés par certains fournisseurs d'antivirus. Ces derniers proposent des outils de génération de posture de sécurité en fonction du nombre de menaces détectées sur l'ensemble des agents déployés.

Grâce aux listes détaillées d'attaques, les membres de l'équipe de tests d'intrusion ont la possibilité de jouir d'une base de connaissance servant de point d'appui et de liste de vérification lors des différents projets de tests d'intrusion.

Pour corroborer les points énoncés précédemment, les intrants de la méthodologie s'inscrivent dans une démarche démarcative et novatrice en ce qui a trait aux sources d'information permettant de déterminer et d'identifier les risques dans l'environnement d'un système d'information.

2.3 Adaptation au contexte de l'environnement

Selon le CASES [10] (Cyberworld Awareness and Security Enhancement Services), lors de la production d'une analyse de risque, il importe en premier lieu de prendre en compte certains critères de base, dont la cible et le périmètre de l'analyse. La définition du contexte décrit notamment l'environnement et l'objet du processus d'évaluation des risques. Le contexte reste une étape indispensable pour comprendre globalement les attentes du client, de façon à adapter la transformation et l'utilisation des résultats de tests d'intrusion.

Les **critères d'évaluation** des risques, selon le CASES, comptent notamment :

- les valeurs stratégiques des processus
- la criticité des actifs
- les exigences légales et contractuelles
- la triade des principes de sécurité CID (confidentialité, intégrité, disponibilité)
- les attentes des parties prenantes et la réputation

Ainsi, pour un service d'authentification sur une plateforme web par exemple, l'importance du critère de confidentialité est supérieure à celui de l'intégrité. Dans certains départements de l'entreprise et de l'environnement client, il y a des risques qu'il faut à tout prix écarter, dans d'autres, il existe des actifs qu'il faut à tout prix protéger. C'est lors de la phase d'évaluation que ces valeurs contextuelles sont définies. Elles doivent être appliquées tout au long de l'analyse des risques.

De ce fait, plusieurs bases de questions ainsi que certains entretiens favorisent une mise en contexte précise sur la portée de l'environnement, la nature des affaires de l'entreprise et les points stratégiques de stockage et transit de l'information sensible et/ou critique.

D'après certains consortiums d'entreprises comme le réseau des grandes entreprises françaises (CIGREF [11]), des mesures et initiatives pour élever leurs niveaux globaux de sécurité informatique sont nécessaires ; l'information est aujourd'hui considérée comme un actif essentiel et stratégique. Depuis 20 ans, la numérisation des documents et actifs de l'entreprise s'est axée vers un idéal d'optimisation de temps et de productivité. Cependant, il s'agit d'un actif intangible, dont la valeur est difficilement mesurable et dont la prise de conscience devrait être amplifiée chez les dirigeants. La majorité des entreprises et des chefs de département font donc face à un paradoxe dans lequel l'accès et la protection de l'information sont jugés stratégiques alors que les budgets et les contrôles sont souvent jugés non prioritaires, par manque de retour sur investissement.

Longtemps, on a considéré que la démarche de protection de l'information « papier » était suffisante, que le fait de ne pas faire transiter d'information sensible par des moyens électroniques,

voire de chiffrer ponctuellement les documents électroniques ou les transmissions, était suffisant. Cependant cette période est révolue depuis très longtemps. Les entreprises ont désormais besoin d'indicateurs précis ainsi que d'une classification dynamique et systématique des actifs informationnels propres à l'entreprise.

Il existe en effet un certain nombre de tendances de fond et de ruptures d'ordre économique, règlementaire et sociologique, qui obligent à repenser de façon plus globale la protection de l'information.

Les États-Unis d'Amérique se dotent dès 2002 d'un cadre régulateur visant à mettre en place une norme de standardisation des informations classées et utilisées dans les agences fédérales. FISMA (Federal Information Security Management Act), permet désormais à l'ensemble des agences américaines de jouir d'une base de référence en ce qui a trait à la classification essentielle de leurs actifs informationnels. L'acte American de 2002, Homeland Security Act [12], permet donc de diriger la tendance mondiale sur la prise de conscience d'une classification effective des actifs informationnels. De plus, cela remet en question et pousse à redéfinir plusieurs processus dans l'entreprise, à savoir :

- Organisationnel
    - Gouvernance de la sécurité et alignement avec la vision d'affaires.
- Ressources humaines
    - Enquête de pré-embauche et surveillance des employés.
- Processus de sécurité
    - Gestion des vulnérabilités, des incidents et des accès.
- Technologie
    - Alignement des plateformes applicatives, systèmes et réseaux avec les contrôles de sécurité.

Un des points saillants de l'analyse du contexte client repose aussi dans la détermination d'un score de maturité en ce qui a trait aux politiques, directives et pratiques de sécurité au sein de l'entreprise.

Le système de classification de maturité du SANS Institute [13] permet de catégoriser 5 types de niveaux de maturité. Ce dernier est un des plus utilisés pour les exercices d'évaluation de maturité, de par la simplicité relative à l'attribution des niveaux en fonction des pratiques et/ou processus évalués. Une des alternatives à ce système de classification est l'échelle COBIT 4.1 [14] reprenant les mêmes principes de catégorisation et ayant un niveau de moins.

Les deux échelles exposées précédemment sont donc utilisées pour quantifier la maturité de l'architecture de sécurité d'une entreprise ou d'un environnement. Elles sont parmi les plus efficaces en termes d'évaluation de maturité.

2.4 Évaluation des risques

Les méthodes actuelles d'évaluation par scénarios sont omniprésentes en entreprise, bien qu'implémentées partiellement ou non maintenues sur une base régulière. Les efforts pour maintenir les méthodologies sont très élevés. La principale raison repose dans le fait que le registre de risque augmente proportionnellement en taille et complexité selon le nombre de scénarios qui le compose. Il faut donc dédier une équipe spécifique à la gestion des risques informatiques. Cette pratique se reflète peu en entreprises, car souvent, par manque de budget ou d'intérêt, les risques sont restreints à un ensemble bien défini de scénarios par défaut qui seront souvent repris lors de l'utilisation de la méthodologie.

Cependant, les approches par scénarios fournissent un bon cheminement méthodologique en ce qui concerne l'attribution des scores de risques ainsi que les recommandations relatives aux risques évalués. Ce sont donc d'excellents intrants, comme le précise R.Oppliger [15], pour reprendre certaines recommandations et les appliquer à certains risques communs en termes de contrôle de traitement. Il est donc nécessaire d'accroître leur efficacité en tenant compte des attaques perpétrées lors du test d'intrusion. Cela permet de sélectionner et de mitiger en priorité des scénarios ayant des vulnérabilités vérifiées de manière tangible.

Certains manufacturiers logiciels se sont aussi, dans les 5 dernières années, spécialisés dans la création de solutions permettant la gestion unifiée des évènements de sécurité. Ces évènements de sécurité sont des journaux générés par des systèmes ou applications comme :

- Évènements de registre Windows
- Sondes IDS / IPS
- Vérificateur d'intégrité des fichiers système
- Solution Antivirale
- Sonde de détection de vulnérabilité

Ces intrants sont ensuite agrégés sur un serveur central permettant d'effectuer des recherches dans la masse de journaux récoltés, tout en créant des indicateurs et diagrammes personnalisés pour représenter la posture de sécurité des actifs informationnels. Cependant, ces solutions logicielles comme *Alien Vault USM* [16] ne permettent pas d'exploiter les vulnérabilités identifiées, ni même de fournir des recommandations spécifiques en fonction des menaces détectées. Elles pourront cependant détecter toute tentative d'intrusion à travers les bases de données, combinées à de la corrélation heuristique.

Il est aussi important de considérer que la majorité des méthodologies par scénarios ont été créées entre les années 1980 et 2000 et que la plupart sont discontinuées, car les contextes et modèles technologiques se sont diversifiés et complexifiés.

D'autres suites logicielles utilisent des concepts très intéressants d'utilisation de détection de vulnérabilités pour venir alimenter un modèle de gestion de la conformité en rapport avec certaines normes de sécurité. Cela permet de savoir quels sont les correctifs et patchs de sécurité manquants ainsi que les systèmes impactés. De plus, pour conserver les contrôles à jour, la solution citée crée des rapports et indicateurs de façon à assurer une traçabilité des évolutions.

Suite à la découverte des différents processus et méthodes exposés à travers la revue de littérature, nous sommes confortés dans notre idée initiale qu'est le développement d'un outil sous forme méthodologique pouvant servir à évaluer et prioriser les risques identifiés par les résultats de tests d'intrusion.

CHAPITRE 3 ITREM — PROCESSUS MÉTHODOLOGIQUE

Pour répondre à la problématique actuelle sur les méthodes et outils disponibles en évaluation des risques appliqués aux résultats de tests d'intrusion, un processus méthodologique a donc été créé. ITREM (Intrusion Testing for Risk Evaluation and Management) est le processus méthodologique que nous avons créé. Ce dernier permet de reprendre les résultats de tests d'intrusion, de façon à les transformer en indicateurs de risque afin de prioriser les traitements.

3.1 Phases de la méthodologie

Le projet de création de méthodologie se scinde en quatre parties distinctes. La figure ci-dessous permet de représenter le passage logique, à haut niveau, entre les différentes parties de la méthodologie. ITREM se décompose en 4 étapes majeures :

1) PTI : Processus de Test d'Intrusion
2) PAC : Processus d'Appréciation du Contexte
3) PER : Processus d'Évaluation des Risques
4) PAMC : Processus d'Amélioration Continue

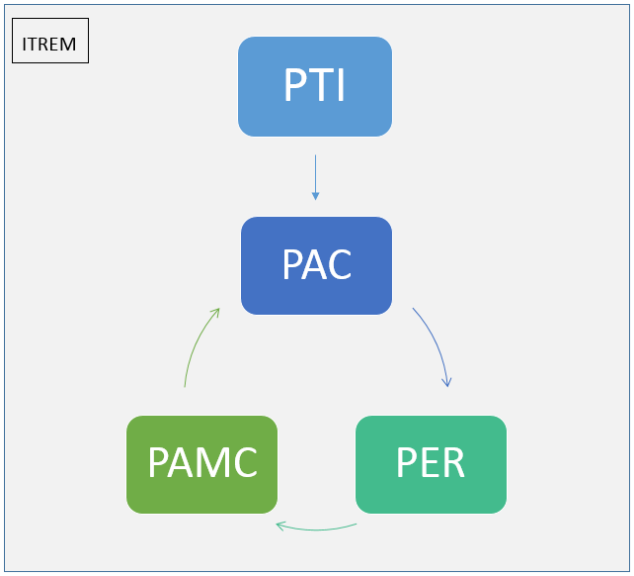

Figure 3-1 Processus cyclique ITREM

Nous allons donc introduire à haut niveau chacune des parties du processus global pour démontrer les liens de causalité entre ces dernières. Par la suite, le corps du chapitre 3 sera scindé en quatre de façon à détailler chacune des parties.

3.1.1 **Processus de tests d'intrusion (PTI)**

Le processus propre au test d'intrusion permet de venir poser des bases stables et reproductibles quant au déroulement des tests effectués sur l'environnement client (EC). Il permet de décrire précisément comment les tests sont effectués et comment les vulnérabilités récoltées seront transposées dans un rapport. Cela entraine une standardisation dans la façon de produire et gérer les résultats relatifs aux tests d'intrusion. La partie de la méthodologie propre aux tests vise à offrir un intrant complet de façon à le transférer au processus d'appréciation du contexte. En effet, un ensemble d'informations détaillées sur les vulnérabilités propre à l'EC sera transmis afin d'être raffiné par le processus d'appréciation.

3.1.2 **Processus d'appréciation du contexte (PAC)**

Le principe d'appréciation du contexte client repose sur la détermination de plusieurs facteurs permettant de venir transformer les résultats des tests d'intrusion. Chaque type d'activité d'intrusion et chaque test sont désormais tracés et répertoriés dans une base de données permettant d'y faire référence. De plus, 4 facteurs déterminants viennent appuyer la nécessité d'une étape de raffinage du contexte :

- L'importance des actifs et leur priorisation dans le cadre du test d'intrusion et selon les spécificités du contexte d'affaires
- Le cadre normatif choisi par le client pour la gestion des risques ou pour les orientations de sécurité
- Les catégories relatives aux fuites d'informations
- La pondération en découlant

3.1.3 **Processus d'évaluation des risques (PER)**

Comme mentionné précédemment dans le chapitre 2, l'évaluation des risques en entreprise se base souvent sur des plateformes méthodologiques prenant en comptes des processus relativement dépassés. Cela est justifié par le fait que les environnements actuels sont de plus en plus exposés aux menaces externes et que les solutions de gestion des risques ne répondent plus adéquatement aux attentes en matière de sécurisation de l'information. Le temps de l'énumération des scénarios, en sécurité informatique, est dépassé.

À l'inverse des processus basés sur l'évaluation de scénarios souvent hypothétiques, nous basons notre processus d'évaluation sur des vulnérabilités provenant d'une liste ayant été créée par le biais du rapport de test d'intrusions et appliquée au contexte d'affaires grâce au PAC. Pour évaluer les vulnérabilités et les risques en découlant, nous allons utiliser une combinaison d'approches quantitatives et qualitatives. Ces dernières permettront d'attribuer un score de risque (analyse quantitative) et un positionnement sur une matrice. De plus, un registre des risques sera créé pour effectuer un suivi constant sur le traitement des risques et leur évolution. De façon à pouvoir obtenir un cycle méthodologique complet et évolutif, il est nécessaire de transférer les résultats de l'évaluation à un processus permettant de les représenter graphiquement. Non seulement cela permet d'effectuer un suivi sur les mesures et contrôles renforcés, mais aussi de cibler des parties de l'EC plus faibles et nécessitant une approche d'évaluation similaire.

3.1.4 **Processus d'amélioration continue (PAMC)**

L'amélioration continue permet de contribuer à un cycle d'évolution constante, comprenant la sécurisation des actifs informationnels du client.

Il vise particulièrement la vérification postérieure des traitements de risque effectués lors de l'étape précédente (PER). De plus, le PAMC permet de fournir plusieurs indicateurs de sécurité basés sur le processus d'évaluation.

Cela permet de constater, à travers le temps, les efforts et moyens ayant été déployés pour contrecarrer et mitiger les risques identifiés. Le processus d'amélioration continue a aussi pour but de reprendre les extrants relatifs au programme de sécurité afin d'implanter un traitement effectif

des vulnérabilités évaluées, un des objectifs finaux étant de pré-conditionner et d'orienter les prochains tests d'intrusion en visant certaines zones d'intérêt dans l'EC. Le Processus d'amélioration continue (PAMC) permet donc d'apporter des améliorations de manière incrémentale ayant pour but de constamment améliorer et consolider la posture de sécurité globale de l'entreprise.

3.2 PTI – Organisation des tests d'intrusion

L'étape d'identification rentre dans le cadre de la recherche active de vulnérabilités sur l'environnement client (EC). Selon la portée des tests, une quantité variable de vulnérabilités va être relevée et reportée dans un fichier conçu à cet effet.

L'identification des vulnérabilités propre à un système d'information est une étape pouvant être effectuée selon deux possibilités :

- Se référer aux connaissances personnelles de l'expert en tests d'intrusion
- Se référer aux bases de données de connaissances d'ITREM disponibles en annexe B et C (Référence à une attaque). Ces annexes sont tirées de bases de vulnérabilités spécifiquement créées pour la méthodologie

Un des problèmes majeurs dans l'identification des vulnérabilités repose dans l'aspect technique très avancé propre aux vulnérabilités et aux risques associés. La conséquence est que les résultats des tests d'intrusions sont souvent assimilés, par les administrateurs d'un EC, comme un intrant difficile à interpréter et à comprendre.

Ci-dessous, nous présentons une vulnérabilité identifiée et concernant des algorithmes non sécuritaires sur un site web exposé publiquement. La figure 3-2 représente des algorithmes de chiffrement faillibles à certaines attaques par collision.

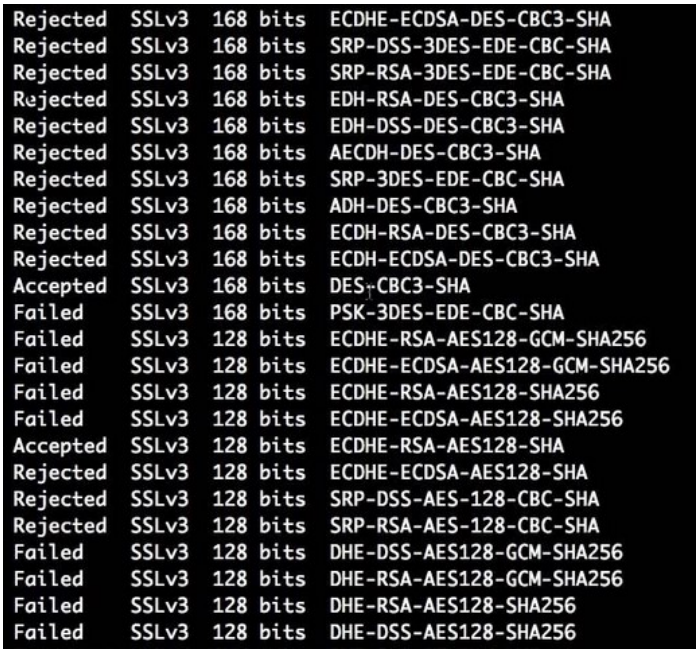

Figure 3-2 Résultats complexes PTI

Il est donc nécessaire de produire une analyse d'impact des vulnérabilités de façon à standardiser les vulnérabilités identifiées.

3.2.1 **Analyse des vulnérabilités**

La partie concernant l'analyse des vulnérabilités est très importante, car elle permet d'effectuer la conversion du risque associé à l'EC, de manière quantitative, en plusieurs données numériques et interprétables. Ce risque se matérialise à travers les vulnérabilités trouvées lors des tests d'intrusion. Il est bien important de comprendre que cette analyse adresse uniquement les risques associés aux vulnérabilités. Pour pallier une approche trop technique et pour éviter tout biais de compréhension, le processus PAC permettra de prendre en compte les paramètres d'affaires jugés nécessaires pour l'étape d'évaluation.

Cela va de pair avec le raisonnement énoncé plus haut, lors de la définition et l'établissement des critères de mesure. Les scénarios adressant des vulnérabilités peuvent aussi être ajoutés, mais cette étape devrait être différenciée de celle adressant les vulnérabilités techniques. De plus, comme mentionné précédemment, il est important d'utiliser cette méthodologie comme une partie venant

ajouter une valeur à l'analyse et à l'appréciation des risques. La prise en compte de l'analyse quantitative permet de concrétiser et préciser le caractère d'impact propre aux menaces, à l'encontre de certaines méthodologies d'analyse de risques qui viendraient souligner cet impact à travers des scénarios et métriques beaucoup plus génériques.

L'analyse des vulnérabilités peut être effectuée grâce aux (CVSS) [17], et peut par la suite être combinée ou convertie par le biais de VANSS (VulnerabilityAnalysis Scoring System), notre propre schéma de pointage de vulnérabilité adapté pour les besoins de notre méthodologie et décrit au chapitre 4. Le but est d'obtenir de façon constante une base standardisée de vulnérabilité, quelle que soit la méthode utilisée. Le processus d'analyse peut cependant débuter directement à travers les chiffriers et calculateurs quantitatifs disponibles pour CVSS et VANSS. L'expert en intrusion peut, dès détection d'une vulnérabilité, utiliser l'outil de calcul et comparer le résultat à la base de données de vulnérabilités (BDOV) pour vérifier si les différents facteurs de calculs sont correctement ordonnancés.

3.2.2 **Composition du rapport**

Les résultats obtenus lors des tests d'intrusion incluent la planification des travaux, l'exécution des tests d'intrusion, l'analyse des résultats et l'identification des solutions. Toutes ces informations seront consolidées à l'intérieur d'un rapport d'analyse qui proposera des recommandations pour contrer les vulnérabilités identifiées. L'approche préconisée ne se limite pas à la remise des données et des rapports produits par les divers outils utilisés lors des tests, mais présente une analyse approfondie des vulnérabilités identifiées pour le domaine d'affaires en plus d'une présentation de solutions concrètes pour corriger ou mitiger les risques associés. Le rapport de vulnérabilité, intrant principal de la méthodologie, est composé de plusieurs parties, dont le rapport créé par l'ETI (Équipe de Test d'Intrusion), Celui-ci permet au client de bénéficier d'une base de référence quant à la sécurité de son environnement, suite aux tests effectués. Le rapport doit être obligatoirement composé des points suivants :

- Un sommaire exécutif comprenant une vision globale de chaque partie du rapport
- La référence aux tests effectués
- Une partie sur les statistiques des concurrents

- Une référence à l'offre de service d'évaluation des risques (selon le client)
- Une partie globale sur les vulnérabilités identifiées
- Une partie détaillée sur les vulnérabilités identifiées

La présentation des vulnérabilités permet d'exposer les résultats de l'analyse de sécurité, détaillée et effectuée par les membres de l'équipe de tests d'intrusions (METI) sur l'environnement client.

Voici comment une vulnérabilité est présentée dans un rapport d'intrusion :

Score CVSS v2 : 5/10 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Vecteur d'attaque	Complexité	Authentification	Impact sur la confidentialité	Impact sur l'intégrité	Impact sur la disponibilité
Local	Élevée	Multiple	Aucun	Aucun	Aucun
Réseau local	Moyenne	Unique	Partiel	Partiel	Partiel
Réseau externe	Faible	Aucune	Complet	Complet	Complet

Figure 3-3 Présentation d'une vulnérabilité

De façon à pouvoir transmettre les vulnérabilités relatives au rapport, il est nécessaire de passer par un processus d'appréciation du contexte.

3.3 PAC – Raffinement des tests et du contexte d'affaires

Il est nécessaire de définir précisément les critères de mesure de risques en tenant compte du contexte de l'entreprise. Pour cela, afin de placer les vulnérabilités sur un ensemble de matrices de classification, que nous désignons l'Ensemble de vulnérabilités ou EV (voir Section 4.1.7.1), une interaction avec le comité client chargé de la sécurité de l'information est nécessaire. Ce dernier comprend le gestionnaire de projet sécurité, le propriétaire de l'actif informationnel, ainsi que tout responsable pouvant apporter une valeur ajoutée dans la détermination des critères.

3.3.1 Contexte et critères

3.3.1.1 Raffinement du contexte

L'Indice de Détection et de Réponse (IDR) permet de cerner la position d'une entreprise relative à sa maturité en termes de sécurité des actifs informationnels sur un environnement spécifique (voir Section 4.1.9). Néanmoins il est nécessaire de développer des considérations plus larges pour mieux cerner le contexte organisationnel global en termes de sécurité informatique. De plus, il est vital d'aligner les objectifs d'affaire d'un client avec la gouvernance propre à la sécurité de ses actifs. Pour cela, l'Équipe de Gestion des Risques (EGR) doit déterminer avec le client les raisons pour lesquelles ce dernier requiert une amélioration de la structure d'évaluation des risques propres à la sécurité informatique. Ce processus de questionnement et d'apprentissage prend tout son sens dans le développement d'une stratégie personnalisée et efficace.

Les raisons peuvent être :

- Mise à jour des politiques de sécurité d'un environnement de système d'information
- Besoin formel en gouvernance sur la sécurité des systèmes d'informations
- Préparation d'un plan de réponse aux incidents
- Préparation d'un plan de continuité des affaires
- Diminution de la surface d'exposition aux attaques
- Énumération des besoins de sécurité pour un environnement spécifique

Par la suite, il est nécessaire de redéfinir des critères de mesures de risques permettant de mieux répondre aux attentes de l'entreprise en rapport avec la sécurité de son information.

3.3.1.2 Définition des critères

Il est à noter que cette méthodologie se distingue par une structure peu commune, car faisant l'objet d'une vision novatrice concernant l'évaluation des risques en entreprise. La notion de critère, utilisée de manière très courante dans la terminologie d'évaluation des risques, vient ici illustrer les critères d'impacts que l'on définit habituellement en début de mandat.

Néanmoins, à l'opposé des techniques d'énumération de scénarios, la question du contexte client dans un test d'intrusion relève ici une très grande importance. La raison repose dans les attentes en rapport avec les tests. Lorsqu'un test d'intrusion est contracté, la majorité du temps, c'est dans le but d'analyser l'EC en reproduisant un mode opérationnel analogue à un attaquant externe et/ou interne. Dans le cadre concernant ce type de test plus communément connu comme BBT (Black Box Testing), la détermination des critères de mesure de risques est très incertaine, subjective et ne donnerait pas de résultats adaptés et précis. Cela est dû principalement à un aspect voulu visant à ce que le responsable de l'EC ne soit pas collaboratif et ne partage aucune information pouvant mener à la découverte de vulnérabilités. Les attentes s'orientent vers une appréciation de la posture de risque de l'EC sans aucune information préalable sauf la portée des adresses IP ou domaines relatifs à l'EC.

ITREM vient donc insérer une dimension des critères de manière complètement singulière, et ce dans le but de répondre correctement aux besoins du client en matière d'expertise technologique et d'orientation relative à la sécurité de son environnement.

Le premier ensemble de critères en rapport direct avec l'EC est celui déterminé de manière générique par VANSS (Vulnerability Analisys Scoring System). Ce sont les indices permettant de caractériser une vulnérabilité avec une valeur numérique. Il est donc important de considérer ces derniers comme des indicateurs techniques sur l'exposition de l'environnement.

Le deuxième ensemble de critères sera propre à l'entreprise cliente et concernera majoritairement les aspects relatifs aux impacts et à la tolérance aux risques. Le client doit donc fournir des indications en rapport avec sa capacité à supporter les différents risques en cas de matérialisation.

Le fait d'avoir une précision de la part du CPM ou du client, permettant de raffiner et de préciser les critères, résulte en une meilleure vision du contexte propre à ce dernier. Cela entraine une amélioration dans l'analyse des vulnérabilités et leurs scores.

Lors de la définition des critères, il est important de déterminer et de prioriser l'importance des critères suivant :

- Critères d'évaluation du risque
- Valeur stratégique de l'information dans le processus d'affaires
- Criticité des actifs informationnels concernés
- Obligations légales et contractuelles (normes, certifications)
- Importance accordée par l'entreprise à la disponibilité, à la confidentialité et à l'intégrité de l'information
- Attente et perception de la direction
- Conséquences négatives sur la réputation

Critères d'impact

- Niveau de classification et de criticité des actifs informationnels
- Perte de confidentialité, intégrité, disponibilité
- Perte d'actifs financiers
- Effets collatéraux
- Atteinte à la réputation

Les critères d'impact sont un reflet des indices utilisés dans VANSS pour déterminer et quantifier l'impact en cas de matérialisation d'une menace sur l'EC. D'autres critères d'impact peuvent être considérés pour mieux apprécier le contexte d'entreprise et sa vision des risques. De cette façon, nous assurons une corrélation entre l'appréciation du risque et son évaluation en prenant une base de critères et d'indices communs.

Par la suite, il est nécessaire de mesurer quantitativement les risques à travers VANSS en modifiant les pondérations d'indices, cela permet ainsi de refléter l'importance des critères pour que le score de risque soit le plus précis possible.

Pour la priorisation et la pondération des facteurs de risque, veuillez vous reporter au chapitre 4.

3.3.2 **Catégories d'entreprise et maturité commune**

Il est important de savoir quelle va être la catégorie d'entreprise ciblée lors des tests de façon à pouvoir appliquer certains ensembles de critères communs, relatifs à la posture de sécurité. Les

entreprises, dépendamment de leur secteur d'activité, auront tendance à présenter des similarités tant au niveau des actifs informationnels qu'aux contre-mesures et processus en assurant la protection.

3.3.2.1 Petite et moyenne entreprise (PME)

Les PME sont de plus en plus nombreuses à prendre conscience de l'importance de la sécurité de l'information. Cependant, par manque de temps, de ressources et de moyens, la sécurité est souvent reléguée en dernier plan.

Les tests d'intrusion sur les environnements de PME permettent :

- D'avoir une meilleure appréciation quant à leur degré de maturité et de réactivité face aux évènements de sécurité.
- D'adapter une offre de service en fonction du processus de test d'intrusion.
    - Fournir du conseil personnalisé quant à la gestion des actifs informationnels et de leur sécurité.
    - Fournir l'opportunité de réduire les profils d'actifs à risque grâce à une méthodologie basée sur des standards internationaux et reconnus à l'échelle mondiale.

3.3.2.2 Grande entreprise

Les grandes entreprises (moins de 5000 employés) ont la plupart du temps des besoins plus spécifiques en rapport avec le PTI. Ces dernières engagent généralement une Équipe de Tests d'Intrusion (ETI) pour répondre à des requis propres à différentes normes et aux certifications associées. Cependant, ces mêmes tests exigés sont généralement basiques et ne couvrent qu'une partie des EC supportant des actifs critiques ou sensibles. Il est donc à leur avantage de continuer ces tests d'intrusion sur d'autres parties de leur plateforme traitant l'information. Les observations constatées lors des phases pilotes de la méthodologie permettent de déduire que ces entreprises détiennent un faible niveau de maturité en ce qui a trait au suivi et au développement futur de leur posture de sécurité.

3.3.2.3 Très grandes entreprises

Les très grandes entreprises (telles que des multinationales), quant à elles, visent plutôt un service de tests d'intrusion complémentaire et à valeur ajoutée. Elles possèdent généralement l'expertise nécessaire à la gestion des actifs informationnels et leur sécurité. Cependant, elles ne détiennent pas une évaluation des risques arrimée avec les tests d'intrusion et cela confirme un constat général faisant état d'un fossé de communication entre les équipes techniques, administrant les systèmes d'information dans l'EC, et les équipes d'évaluation des risques, s'occupant de l'énumération des scénarios jusqu'au traitement des risques.

Une fois que l'appréciation du contexte est effectuée à travers la compréhension de l'EC et de la détermination des poids des critères de mesure, il est possible de passer à l'étape d'évaluation des risques relatifs à l'EC.

3.4 PER – Évaluation des risques

La gestion du risque vise à identifier et anticiper les évènements, actions ou inactions susceptibles d'impacter la mise en œuvre de la stratégie de sécurité informatique sur un horizon donné. La gestion va aussi définir les options de traitement et assurer que les mesures de mitigation appropriées soient choisies, puis mettre en œuvre cette option et contrôler l'efficacité de la solution retenue par rapport aux attentes sur le domaine d'affaires concerné. L'évaluation des risques est régie par les étapes d'établissement du contexte, de détermination des critères de mesures, d'évaluation des vulnérabilités et risques associés, ainsi que par le traitement à travers un plan d'action.

Ces étapes, bien que génériques et reprises dans de nombreuses méthodologies, peuvent être modifiées pour apporter une dimension de personnalisation et d'adaptation. Il est à préciser que la méthodologie créée permet de venir adapter l'évaluation des risques selon la portée de l'EC, sur lequel les tests d'intrusion ont été conduits.

La fusion entre les tests d'intrusion et l'évaluation des risques permet de créer une valeur notoire sur le marché très complexe et varié concernant la protection des données en entreprises. En effet, le processus d'intrusion s'assimile à un intrant très précis et factuel, en grande partie dû au fait que

ce dernier reflète concrètement les attaques et tests réels sur une infrastructure numérique composée de plusieurs équipements et progiciels. La méthodologie vient donc se placer comme un processus complémentaire et mélioratif par rapport aux autres types de méthodes d'énumération de scénarios hypothétiques.

VANSS sera le moteur principal pour l'évaluation et la représentation des risques relatifs à un EC. À cet effet, vous pouvez vous reporter directement au chapitre 4 pour l'analyse détaillée du moteur d'évaluation des risques.

3.5 PAMC – Apprentissage organisationnel

Comme le mentionne Jacques Leplat, dans son ouvrage dédié à l'apprentissage organisationnel (A.O.) [18], le schéma générique de l'A.O. comprend :

- un contenu d'information ou *produit d'apprentissage* (vulnérabilités et risques associés);
- un processus *d'apprentissage* qui consiste à acquérir, traiter et stocker l'information ;
- un *apprenant* (l'entreprise) à qui le processus d'apprentissage profite.

Ces trois points, soutenant l'apprentissage organisationnel, permettent d'initier le cycle continu que nous désirons inscrire dans le processus méthodologique d'ITREM.

En effet, nous désirons créer des indicateurs précis permettant à l'entreprise de conserver une traçabilité des tests effectués, des risques évalués et des traitements appliqués.

Le contenu du produit d'apprentissage se rapporte principalement aux différents tests d'intrusions et à la portée de ces derniers. À cet effet, il est nécessaire de conserver deux types de données :

- La portée des tests ainsi que les vulnérabilités trouvées sur un EC.
- Toutes les vulnérabilités propres à une catégorie d'affaires (CAF).

Cela permet de constituer des bases servant de référence, tant pour l'entreprise requérant une identification et évaluation des risques que pour la méthodologie visant à conserver une traçabilité des tests et risques relatifs pour chaque entreprise dans une catégorie d'affaires.

Le processus d'amélioration continu permettra, à long terme, de conforter et faire évoluer les bases de vulnérabilités ainsi que les indicateurs sous-jacents. C'est le processus permettant de reconduire le cycle de gestion des risques vers la prise de contexte et l'identification des vulnérabilités sur des nouveaux segments de l'environnement numérique.

CHAPITRE 4 ITREM — ANALYSE TECHNIQUE

4.1 VANSS

4.1.1 Introduction à VANSS

Le *Vulnerability Analysis Scoring System*, ou VANSS, est un système composé de plusieurs métriques, servant à analyser les vulnérabilités dans le cadre de la méthodologie ITREM. La méthodologie VANSS s'imbrique dans un processus d'évaluation des risques et vient plus particulièrement se placer après l'étape d'identification des vulnérabilités.

Nous allons définir à travers ce processus de traitement de vulnérabilités les différentes mesures permettant d'apporter une valeur déterministe, novatrice et différente de CVSS. Les mesures définies dans ce document devront être utilisées en parallèle avec CVSS. Elles permettent d'influencer les décisions qui vont découler de l'étape d'analyse des risques.

VANSS permet de répondre à plusieurs objectifs et d'adresser plusieurs besoins nécessaires à la bonne conduite d'une analyse de risques.

En premier lieu, c'est une plateforme d'analyse adaptable. En effet les différents facteurs que nous exposons permettent d'être adaptés et modulés en fonction des profils d'analyse. Ces profils permettent de catégoriser les environnements sur lesquels les analyses seront effectuées. Les règles de pondération peuvent donc être adaptées en fonction du besoin, du contexte de l'EC et des environnements similaires.

Par ailleurs, la comparaison des facteurs et des risques permet de son côté à chaque vulnérabilité identifiée d'être caractérisée en fonction de différents facteurs représentant eux-mêmes plusieurs indices :

- 4 facteurs
- 16 indices
- 75 paliers

4.1.2 **Définition des risques et mécanique des mesures**

4.1.2.1 Risques

Les risques définis à travers cette méthode sont tous associés à une ou plusieurs vulnérabilités identifiées précédemment dans l'étape comprenant les tests sur les infrastructures de données.

L'identification des vulnérabilités permet donc d'obtenir un ensemble de failles exploitées chacune par une ou plusieurs menaces potentielles et une atteinte aux principes de confidentialité, d'intégrité et de disponibilité.

La méthode actuelle utilisée lors des tests d'intrusion et pour l'analyse des vulnérabilités est CVSS. Elle permet d'apporter une approche standardisée et de calculer les scores d'impact sur une échelle de 0 à 10 (0 indiquant un impact extrêmement faible et 10 un impact extrêmement élevé en cas de matérialisation de la menace). La métrique CVSS de base (composée de 6 facteurs) ne donne malheureusement pas d'information sur les tendances, l'environnement du client, et les facteurs de menaces externes. C'est en se basant sur ces intrants manquants, sur notre vision de la sécurité, ainsi que sur l'analyse d'autres méthodologies et mesures que nous allons créer de nouvelles mesures.

Les mesures que nous allons exposer dans ce document vont permettre d'obtenir d'autres valeurs numériques permettant de faire correspondre des niveaux d'exposition propres aux caractéristiques des vulnérabilités. De plus, ces mesures seront utilisées en parallèle avec celles de CVSS.

4.1.2.2 Mécanique des mesures

Les facteurs propres aux mesures seront détaillés dans les parties 3, 4 et 5 de cette section. Le but de cette partie est d'exposer globalement ces dernières et de montrer comment elles interagissent entre elles dans la détermination des scores. Les détails concernant les calculs seront exposés dans la partie 6.

Il est important de considérer les termes suivants pour la lecture de la suite de ce document.

Mesures. Les mesures représentent les différents ensembles majeurs de cette méthodologie d'analyse des risques. Elles rassemblent les différents facteurs et permettent d'obtenir un score de risque unique pour chacune d'entre elles.

Facteurs. Ces derniers sont intrinsèquement liés aux mesures. Ils expriment les caractéristiques de chacune. Par exemple, pour une mesure de potentialité, un des facteurs déterminants sera l'exploitation. Chaque facteur est détaillé lorsqu'une nouvelle mesure est exposée. De plus, les facteurs peuvent être pondérés pour accorder une priorisation plus ou moins importante selon le contexte client et l'environnement sur lequel reposent les actifs informationnels.

Indice. Les indices sont les sous-ensembles des mesures, ils viennent représenter numériquement les risques propres à chaque vulnérabilité identifiée. Pour cela, ils sont composés de paliers qui servent à énumérer et concrétiser les valeurs numériques caractérisant chaque vulnérabilité.

Veuillez trouver ci-dessous le tableau représentant le modèle permettant d'illustrer chaque facteur.

Tableau 4-1 Modèle d'un facteur de potentialité ou d'impact

Facteur modèle			
Indice 1	Indice 2	Indice 3	Indice 4
Valeur palier	Valeur palier	Valeur palier	Valeur palier
Score pour le facteur			

4.1.3 Échelle de calcul des risques

L'échelle de calcul des risques de VANSS, une fois les vulnérabilités identifiées, est calquée sur le même intervalle que CVSS. À savoir :

- 0 pour un impact ou potentialité inexistant(e).
- 10 pour un impact ou potentialité imminent(e).

Le passage entre 0 et 10 se fait principalement à travers 5 niveaux et grâce à une incrémentation d'une valeur quantitative de 2 unités.

Cette échelle est inspirée de la norme ISO/IEC 31000:2009 intitulée « Management du risque — Principes et lignes directrices » [19].

4.1.4 Mesures de potentialité

Une fois que le testeur a identifié un risque potentiel et veut quantifier la gravité attenante, la première étape consiste à estimer sa « potentialité ». La façon de le faire est d'estimer une mesure de la potentialité liée à la vulnérabilité. Cette estimation repose sur une prémisse tenant en compte que la faille est découverte et exploitée par l'attaquant. Il est nécessaire d'être précis avec les estimations lors de l'analyse de l'environnement client de manière à avoir le maximum de cohérence dans le calcul des scores de risque.

De nombreux indices permettent d'estimer la potentialité. Nous allons catégoriser ces indices de potentialité en deux catégories de facteurs.

4.1.4.1 Facteur d'agent de menace

Le but de ce facteur est d'estimer précisément, grâce aux tests d'intrusion, les groupes d'attaquants susceptibles de mener une/des attaques avec succès. Il est à noter que les résultats des tests d'intrusion, effectués précédemment, permettent d'avoir une vision très claire et précise sur l'ensemble des failles présentes sur l'environnement. De plus, l'équipe responsable du processus d'intrusion est expérimentée et vraisemblablement dans une position clé pour visualiser les différents acteurs afférents aux vulnérabilités et capables de les exploiter.

Les indices propres au facteur d'agents de menace sont quantifiés sur une échelle de 0 à 10.

La pondération de chaque indice permet de quantifier le niveau de criticité en relation avec la potentialité liée aux vulnérabilités. Le score de chaque indice est indiqué entre parenthèses à la fin de chaque niveau.

4.1.4.1.1 Indice de niveau de compétence (INC)

Le niveau de compétence indique les qualifications de l'agent de menace. Ces qualifications s'apparentent aux connaissances de l'agent en matière de tests d'intrusion et de recherche spécialisée en vulnérabilité.

- L'indice compte ici 6 paliers :
    - Expert en recherche de vulnérabilité (10)
    - Spécialiste en tests d'intrusion (8)
    - Bonne connaissance en programmation, réseau et système (6)
    - Utilisateur avancé (4)
    - Connaissance partielle de l'informatique (2)
    - Pas de connaissance technique en informatique (0)

4.1.4.1.2 Indice de motivation (IMO)

À quel point la compagnie ou l'environnement représente-t-il un intérêt pour le groupe d'agents ? Quelles sont les motivations pouvant entrainer une exploitation de la faille ? (propriété intellectuelle, carte de crédit, gouvernement, informations secrètes, etc.)

- L'indice compte ici 4 paliers :
    - Intérêt très important (8)
    - Intérêt important (6)
    - Intérêt moyen (4)
    - Intérêt faible (2)

4.1.4.1.3 Indice d'opportunité (IOP)

L'indice d'opportunité concerne les vecteurs d'accès et les ressources nécessaires pour exploiter la vulnérabilité.

- L'indice compte ici 4 paliers :
    - Pas d'accès précis ou de ressources financières particulières (8)
    - Accès particulier ou ressources financières modérées (6)
    - Accès spécial ou ressources financières élevées (4)
    - Accès complet ou ressources financières très élevées (2)

4.1.4.1.4 Indice de population de l'agent (IPA)

Quelle est la caractéristique du groupe représentant l'agent de menace ?

- L'indice compte ici 5 paliers :

- Utilisateur anonyme (10)
- Utilisateur authentifié (8)
- Utilisateur de réseaux partenaires (6)
- Utilisateur du réseau interne (4)
- Développeur/Administrateur (2)

4.1.4.2 Facteur de Vulnérabilité

Le but du facteur de vulnérabilité est d'apporter grâce aux différents indices les caractéristiques et la quantification des aspects propres aux failles.

Les indices liés au facteur de vulnérabilité sont quantifiés sur une échelle de 0 à 10. La pondération de chaque indice permet de représenter le niveau de criticité en relation avec la découverte et l'exploitation des vulnérabilités.

4.1.4.2.1 Indice de découverte (IDE)

L'indice de découverte permet d'induire le niveau de difficulté nécessaire à la découverte de la vulnérabilité.

- L'indice compte ici 5 paliers :
  - Outils automatisés disponibles, très faciles (10)
  - Modèle, type ou code de vulnérabilité disponible, facile (8)
  - Utilisation de tests de données aléatoires ou « fuzzing », difficulté modérée (6)
  - Difficile (4)
  - Quasiment impossible (2)

4.1.4.2.2 Indice d'exploitation (IEP)

L'indice d'exploitation permet de préciser le niveau de difficulté nécessaire à l'exploitation de la vulnérabilité.

- L'indice compte ici 5 paliers :
  - Outils automatisés disponibles, très facile (10)
  - Exploit disponible (8)

- Exploit facile à créer (6)
- Exploit difficile à créer (4)
- Exploitation théorique (2)

4.1.5 **Mesure d'impact**

Lorsque nous arrivons à l'étape d'énumérer et calculer les mesures d'impact, il est important de considérer deux types de répercussions importantes. La première représente le facteur d'impact technique. La deuxième, le facteur impact d'affaires.

L'impact technique vient toucher l'application, le réseau, le système, les données présentes et les fonctionnalités majeures.

L'impact d'affaires vient quant à lui se placer après le facteur technique et requiert une bonne compréhension du contexte d'affaires de l'entreprise et des impacts financiers liés aux systèmes d'information. Il est à noter que les informations financières peuvent ne pas être accessibles. Il convient donc de poser des hypothèses en supposant des plafonds d'impacts, ou de produire le plus de détails techniques de telle manière à ce que les responsables du mandat puissent prendre une décision sur les indices d'affaires.

4.1.5.1 Facteur d'impact technique

4.1.5.1.1 Indice de type de données (ITP)

L'indice de type de données permet d'avoir un échelonnage sur le degré de criticité propre aux informations accessibles via la vulnérabilité exploitée.

- L'indice compte ici 5 paliers :
    - Critique (10)
    - Sensible (8)
      Exemple : Numéros de sécurité sociale d'employés, numéros de cartes de crédit
    - Privée (6)
      Exemple : Contrats avec des fournisseurs, revenus d'employés
    - Interne (4)
      Exemple : Directives de vente, organigrammes
    - Publique (2)

4.1.5.1.2 Indice de vecteur d'attaque (IVA)

L'indice de vecteur d'attaque permet de déterminer depuis quelle zone la vulnérabilité a été identifiée.

- L'indice compte ici 4 paliers :
    - Accès externe (8)
    - Accès adjacent (6)
    - Accès interne (4)
    - Compte local (2)

4.1.5.1.3 Indice de perte de confidentialité (IPC) :

L'indice de perte de confidentialité permet d'avoir un niveau plus précis que celui utilisé dans la mesure de base de CVSS.

- L'indice compte ici 6 paliers :
    - Toutes les données critiques sont divulguées (10)
    - Toutes les données non critiques sont divulguées (8)
    - Une partie notable des données sensibles est divulguée (6)
    - Une partie notable des données non sensibles est divulguée (4)
    - Une partie minime des données sensibles est divulguée (2)
    - Une partie minime des données non sensibles est divulguée (1)

4.1.5.1.4 Indice de perte d'intégrité (IPI)

L'indice de perte d'intégrité permet d'avoir un niveau plus précis que celui utilisé dans la mesure de base de CVSS.

- L'indice compte ici 4 paliers :
    - Toutes les données critiques sont corrompues (10)
    - Toutes les données non critiques sont corrompues (8)
    - Une partie notable des données sensibles est corrompue (8)
    - Une partie notable des données non sensibles est corrompue (6)

- Une partie minime des données sensibles est corrompue (6)
- Une partie minime des données non sensibles est corrompue (2)

4.1.5.1.5 Indice de perte de disponibilité (IPD)

L'indice de perte de disponibilité permet d'avoir un niveau plus précis que celui utilisé dans la mesure de base de CVSS.

- L'indice compte ici 5 paliers :
  - Tous les services en ligne et à l'interne sont indisponibles pour une durée indéterminée (10)
  - Tous les services à l'interne sont indisponibles (8)
  - Tous les services en ligne sont indisponibles (8)
  - Une partie des services primaires à l'interne est indisponible (6)
  - Une partie des services primaires en ligne est indisponible (6)
  - Courte interruption des services internes (<24H) (4)
  - Courte interruption des services en ligne (<24H) (4)
  - Interruption minime (2)

4.1.5.2 Facteur d'impact d'affaires

4.1.5.2.1 Indice de dommages financiers (IDF)

L'indice de dommage financier permet de quantifier la perte financière, en termes de pourcentage du Chiffre d'Affaire (CA), liée à l'exploitation de la vulnérabilité.

- L'indice compte ici 6 paliers :
  - Banqueroute, perte totale (10)
  - Perte de plus de 75 % du CA (8)
  - Perte entre 50 et 75 % du CA (6)
  - Perte entre 25 % et 50 % du CA (4)
  - Effet mineur sur le CA (2)
  - Coût permettant de fixer la vulnérabilité (1)

- Moins que le coût nécessaire à fixer la vulnérabilité (1)

4.1.5.2.2 Indice de dommage de réputation (IDR)

L'indice de dommage lié à la réputation permet de quantifier les dommages propres à l'image de la marque et/ou de l'entreprise.

- L'indice compte ici 5 paliers :
  - Dommage prononcé, atteinte à la marque et à l'entreprise (10)
  - Perte de plus de 25 % de la clientèle et/ou perte de 10% ou plus du CA (8)
  - Propagation notable sur les réseaux sociaux (6)
  - Perte de clients majeurs (4)
  - Dommage minime (2)

4.1.5.2.3 Indice d'information privée (IIP)

L'indice permet de quantifier globalement le nombre de personnes impactées par l'accès à des données personnelles.

- L'indice compte ici 5 paliers :
  - < 1 M (10)
  - Entre 100K et 1M (8)
  - Entre 10K et 100K (6)
  - Entre 1K et 10K (4)
  - Entre 100 et 1K (4)
  - Moins de 100 (2)

4.1.6 Calcul des scores de risques

4.1.6.1 Aide à la décision

Les méthodes concernant l'aide à la décision sont nombreuses et se focalisent principalement sur une approche scientifique permettant de résoudre les problèmes de décision applicables à une multitude de contextes. Dans notre cas actuel, l'aide à la décision passe par une méthode de calcul

prenant comme base les sommes pondérées des différents indices VANSS pour produire un score de vulnérabilité en accord avec la réalité de l'EC.

Pour corroborer le vocabulaire utilisé dans les analyses multicritères, nous faisons face à une situation où il est nécessaire de créer une modélisation des vulnérabilités, et ce dans le cas d'une problématique de tri. Pour cette analyse, il est impératif de prendre en compte des critères qui serviront aux calculs et à la transformation numérique des valeurs associées aux indices. Nous évoluons donc dans un cadre ouvert de réflexion, où le but tend vers un modèle d'investigation et de solutions concernant les vulnérabilités.

4.1.6.2 Pondération

La pondération est une étape très importante dans l'appréciation et la notation des risques. Les scores de vulnérabilité seront influencés par cette pondération et il est donc nécessaire de la choisir de façon adaptée pour les calculs. Pour cela, vous pouvez vous référer au tableau ci-dessous pour prendre référence des pondérations établies selon les indices.

Tableau 4-2 Poids et comparaison des critères

Comparaison des critères (Indices)	Poids
Importance égale de deux éléments	**10**
Faible importance d'un élément par rapport à un autre	**30**
Importance forte d'un élément par rapport à un autre	**50**
Importance attestée d'un élément par rapport à un autre	**70**

Les critères sont ici assimilés aux indices. Au total, VANSS compte 14 indices et 4 facteurs propres aux mesures de potentialité et d'impact. Un critère doit permettre de mesurer et refléter les préférences du décideur en rapport avec chaque vulnérabilité. Ci-dessous, nous présentons la formule permettant de calculer le score de risque de chaque vulnérabilité en fonction des critères. Elle doit être interprétée comme la somme de la valeur de chaque critère (indice) multipliée par la valeur de chaque poids.

$$V(v_i) = \sum_{j}^{n} w_j \, v_{ij} \quad , \ \forall i \in [1,n] \qquad (1)$$

Dans l'équation ci-dessus, les variables sont définies comme telles :

- $V(v_i)$ Valeur du score de risque. La valeur du score de risque est composée de 3 chiffres significatifs.
- w_j Valeur du poids pour le critère / indice. La valeur est composée de 2 chiffres significatifs.
- v_{ij} Valeur normalisée de l'indice. La valeur est composée d'un chiffre significatif.

Voici donc les indices et facteurs que l'on considérera comme critères dans la suite de l'explication de la méthodologie.

Les facteurs sont regroupés en 4 catégories :

- Facteur d'Agent de Menace (FAM)
- Facteur de Vulnérabilité (FV)
- Facteur d'Impact Technique (FIT)
- Facteur d'impact Affaires (FA)

Tableau 4-3 Tableau des facteurs et indices

Calculateur vulnérabilité	INC	IMO	IOP	IPA	IDE	IEP	ITP	IVA	IPC	IPI	IPD	IDF	IDR	IIP	TOT
Facteurs	FAM (40)				FV (20)		FIT (50)					FA (30)			
Pondération Facteurs	40				20		50					30			140
Pondération Indice	10	10	10	10	10	10	10	10	10	10	10	10	10	10	140

Comme expliqué précédemment, le but est que les Membres de l'Équipe de Test d'Intrusion (METI) tirent profit de la connaissance acquise sur l'EC pour ajuster les différentes pondérations. Cependant, ils peuvent toujours prendre leurs références et utiliser les différents modèles clients où les pondérations sont déjà calculées, et servent à produire les scores plus rapidement. Cela facilite la tâche pour l'analyse.

Comme décrit dans le tableau ci-dessus, la somme des facteurs et la somme des indices doivent être supérieures à 140. La répartition de la pondération par facteur est donc importante, car privilégier un facteur implique forcément d'en diminuer un autre.

$$\sum_{1}^{n} \boldsymbol{w_j} \geq \mathbf{140} \quad , \quad \forall \boldsymbol{j} \in [\mathbf{1}, \boldsymbol{n}] \qquad \textbf{(2)}$$

4.1.6.3 Normalisation

La normalisation des poids permet de vérifier que la somme des indices ne peut dépasser la valeur de risque maximale (10), tout en tenant compte de la pondération appliquée. Pour cela, nous divisons chaque valeur propre aux critères de vulnérabilités par la somme totale des valeurs.

$$\boldsymbol{v_{ij}} = \frac{\boldsymbol{v_i}}{\sum_{\boldsymbol{i}} \boldsymbol{a_i}} \quad , \forall \boldsymbol{i} \in [\mathbf{1}, \boldsymbol{n}] \qquad \textbf{(3)}$$

Dans l'équation ci-dessus, les variables sont définies comme telles :

- v_{ij} Valeur normalisée pour chaque indice. Cette valeur ne comporte qu'un seul chiffre significatif.
- v_i Valeur de l'indice sans normalisation
- a_i Somme des indices sans normalisation

Voici un exemple concret :

Si je détermine que deux de mes indices sont plus importants que le reste, nous allons donc les pondérer en accord et voir l'impact sur le score de risque.

Ci-dessous, le tableau avec une pondération équirépartie.

Tableau 4-4 Pondération équirépartie

Calculateur vulnérabilité	INC	IMO	IOP	IPA	IDE	IEP	ITP	ISI	IPC	IPI	IPD	IDF	IDR	IIP	TOT
Facteurs	FAM (38)				FV (22)		FIT (45)					FA (35)			
Pondération / Facteur	40				20		50					30			140
Pondération / Indice	10	10	10	10	10	10	10	10	10	10	10	10	10	10	140
Vulnérabilité 1	10	4	6	4	4	6	6	6	10	10	8	10	10	10	140
	0.1	0.03	0	0.03	0	0	0	0	0.1	0.1	0.06	0.07	0.07	0.1	7.43

Il est important de préciser que les scores de risque obtenus, ainsi que les scores pour les indices, sont systématiquement arrondis au centième.

Les valeurs normalisées sont surlignées en jaune et les valeurs sans normalisation sont en orange. On distingue bien ici que chaque critère est divisé par 140, représentant la somme totale des poids pour chacun des indices propres à la vulnérabilité.

Ci-dessous, deux indices vont bénéficier d'une priorisation. Ces derniers seront IPD (Indice de Perte de Disponibilité) et IDF (Indice de Dommage Financier). Nous allons leur attribuer une pondération de 50 chacun.

Tableau 4-5 Normalisation avec une pondération non linéaire

Calculateur vulnérabilité	INC	IMO	IOP	IPA	IDE	IEP	ITP	ISI	IPC	IPI	IPD	IDF	IDR	IIP	TOT
Facteurs	FAM (38)				FV (22)		FIT (45)					FA (35)			
Pondération / Facteur	40				20		90					70			220
Pondération / Indice	10	10	10	10	10	10	10	10	10	10	50	50	10	10	220
Vulnérabilité 1	10	4	6	4	4	6	6	6	10	10	8	10	10	10	220
	0	0.02	0	0.02	0	0	0	0.03	0	0	0.04	0.05	0.05	0	8

Comme on peut le constater, la somme des pondérations a changé. La normalisation a permis de prendre en compte les deux indices prioritaires, tout en changeant légèrement le score de risque. La valeur du score de risque est donc 8,00 / 10.

On distingue bien ici que chaque critère est divisé par 220, représentant la somme totale des poids pour chacun des indices propres à la vulnérabilité.

4.1.6.4 Calcul des scores de vulnérabilités

Chaque vulnérabilité est par la suite calculée en faisant la somme des valeurs normalisées multipliées par le poids des critères.

On obtient par la suite le score de risque associé.

Tableau 4-6 Calcul du risque

Vulnérabilité 1	10	4	6	4	4	6	6	6	10	10	8	10	10	10	140
	0.07	0.03	0.04	0.03	0.03	0.04	0.04	0.04	0.1	0.1	0.06	0.07	0.07	0.1	7.43

Il est très important de considérer que le calcul des scores de risques est dépendant des critères et de leur pondération.

4.1.7 GIPS (Gestion des Indicateurs de Posture de Sécurité)

La gestion des indicateurs de posture de sécurité (GIPS) comprend la création, le développement et l'évolution des indicateurs. Ces derniers sont produits dans le but de fournir un niveau d'abstraction plus élevé en rapport avec les vulnérabilités trouvées et analysées sur l'environnement client. De plus, ils permettent de fournir des données sur les groupes de vulnérabilités propres au client. Ceci va permettre par la suite à l'EGR de reprendre les différents ensembles et d'émettre un plan de correctifs en accord avec la posture. L'étape propre à GIPS est la dernière à laquelle le METI doit prendre part en tant qu'acteur principal de la méthodologie.

4.1.7.1 BDOV (Base de Donnée Orientée Vulnérabilité)

Les vulnérabilités relevées dans les EC doivent être analysées, puis classées et réparties selon la catégorie d'affaires à laquelle appartient l'EC. Pour cela, sachant que chaque mandat client donne lieu à des ensembles de vulnérabilités uniques, nous introduisons la notion de Base de Donnée Orientée Vulnérabilité (BDOV).

Les BDOV sont les bases répertoriant toutes les vulnérabilités des EC. Chaque BDOV est unique de par le nombre et le type de vulnérabilités la caractérisant. Ce système de classification des vulnérabilités permet de donner à GIPS toute la matière nécessaire à la création des indicateurs de sécurité. À partir des données récoltées sur les EC et traduites numériquement à travers VANSS, il est avantageux de créer des indicateurs statistiques qui permettront de fournir une dimension de suivi personnalisé pour chaque client. Il faut garder en tête qu'aucune donnée relative au client, et pouvant mener à son identification, ne pourra être dévoilée. Pour cela, chaque BDOV devra être identifiée par un ID unique permettant d'y faire référence.

Les BDOV vont se situer à deux niveaux dans notre méthodologie.

- Premièrement une BDOV propre à chaque test effectué.
- Un RDV (Registre Dédié aux Vulnérabilités) venant regrouper toutes les BDOV propres à chaque famille et/ou secteur d'affaires (Financier, universitaire, gouvernemental, etc.). Les vulnérabilités et surfaces d'attaque seront similaires de par les choix technologiques communs utilisés pour traiter des actifs similaires.

Les BDOV sont composées de toutes les vulnérabilités trouvées et analysées sur un EC. Une fois que le METI a attribué un score à chaque vulnérabilité, il est important de classer ces dernières par ensembles de vulnérabilités (EV). La notion d'EV est un des points clés de la méthodologie, car elle permet de réunir plusieurs vulnérabilités impactant les mêmes composants, équipements, logiciels ou domaines. Par exemple un EV peut correspondre à la zone réseau externe, les postes de travail utilisateurs, les serveurs applicatifs, etc. Ils sont généralement dépendants du mandat et de la portée de ce dernier. Les catégories d'EV seront exposées dans chaque BDOV pour que le METI puisse y faire référence et procéder à la classification.

Une fois cette étape de classification achevée, les EV peuvent être révisés par un pair, contribuant à une double vérification quant à la justesse de classification des vulnérabilités dans les EV. Une fois les EV constitués, les statistiques et profils propres aux risques associés seront calculés en fonction des vulnérabilités contenues dans chaque ensemble. Les METI peuvent ensuite donner leur recommandation par vulnérabilité et par EV. Plusieurs illustrations, présentées ci-dessous,

permettront de mieux représenter les BDOV, VOD et les interactions dans la partie d'analyse des vulnérabilités.

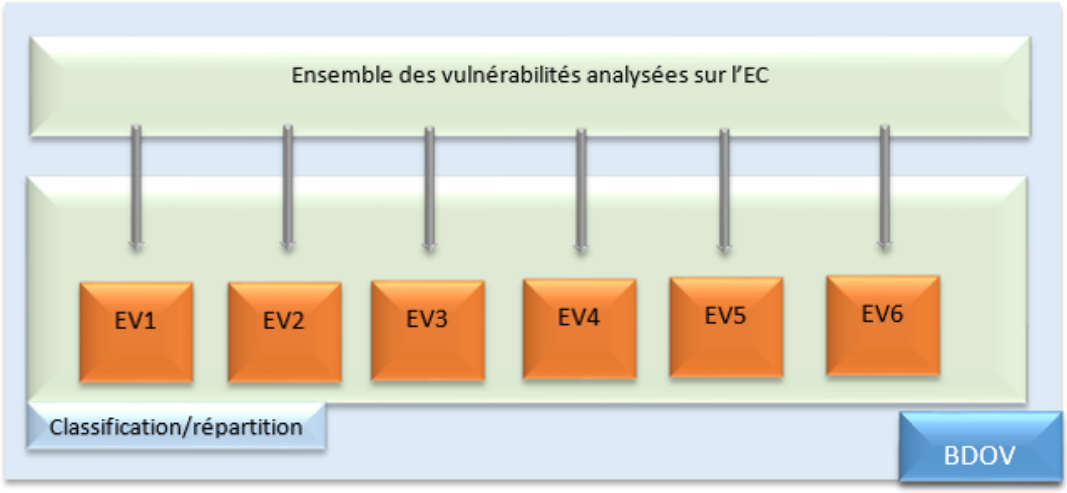

Figure 4-1 BDOV – Base de données orientée vulnérabilité

Les RDV (Répertoires Dédiés aux Vulnérabilités) sont simplement les dossiers, chiffriers ou bases de données répertoriant toutes les BDOV par catégorie d'affaires (CAF). Cela permet d'obtenir plusieurs informations d'ordre comparatif, par rapport aux tendances de menace sur le marché de la sécurité des technologies de l'information et par types de CAF. La criticité des informations est potentiellement similaire selon les catégories d'affaires.

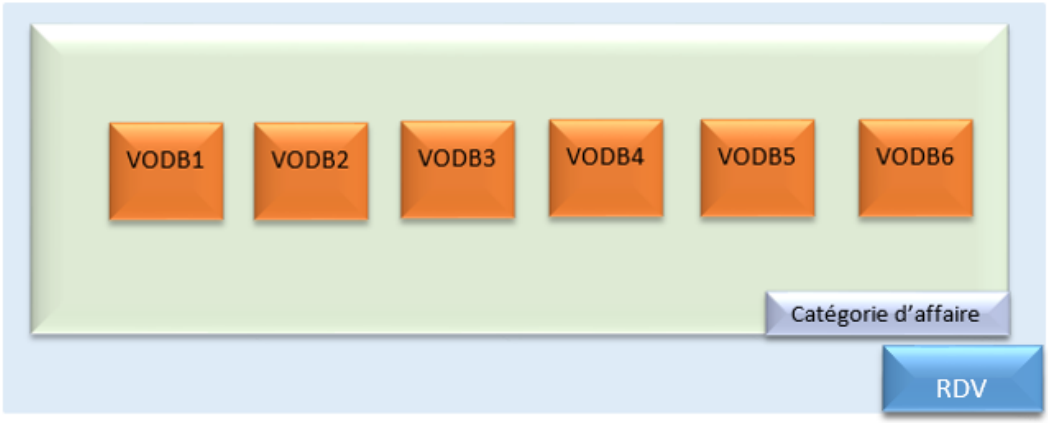

Figure 4-2 RDV - Répertoire dédié aux vulnérabilités

4.1.8 EV (Ensemble de vulnérabilités)

Les ensembles de vulnérabilités représentent un élément clé de cette méthodologie. Ils permettent de classer les vulnérabilités, mais surtout ils guident les MEGR (Membre de l'Équipe de Gestion des Risques) vers les catégories de contrôle et de contre-mesures à implanter lors de l'étape de traitement. Un EV n'est autre qu'un groupe de vulnérabilités pouvant se rattacher à une catégorie de contrôle. La raison repose dans le traitement et les contre-mesures. Si une vulnérabilité est réduite par un contrôle, il est fort probable que le contrôle en question puisse aussi réduire la posture de risque pour d'autres vulnérabilités se rapportant à la même catégorie de contrôle. Lorsqu'un METI regroupe les vulnérabilités d'un EC, il se doit de le faire en prenant les 32 catégories de contrôle propres à ISO/IEC 27002 :2013 [20], intitulées « Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information ».

Voici quelques-unes des catégories avec lesquelles les METI et MEGR doivent associer les vulnérabilités de l'EC.

Tableau 4-7 EV - Ensemble de vulnérabilité

Réf.	Ensemble de vulnérabilité	Objectifs
5.1	**Orientations de la direction en matière de sécurité de l'information**	Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.
6.1	**Organisation interne**	Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation.
6.2	**Appareils mobiles et télétravail**	Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.
8.1	**Responsabilités relatives aux actifs**	Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée.

Tableau 4-7 EV - Ensemble de vulnérabilité

8.2	**Classification de l'information**	S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.

Désormais, il est primordial de définir en quoi les bases de données de vulnérabilités vont servir de source pour GIPS. L'IDR (Indice de Détection et de Réponse) et les indicateurs de posture vont permettre de répondre à ce besoin. Pour cela, la prochaine sous-partie va nous permettre d'introduire ces différentes notions.

4.1.9 IDR (Indice de Détection et de Réponse)

Les indicateurs de détection et de réponse permettent aux METI de mieux apprécier les réactions du client lors des tests. Il est à noter que cette étape est facultative et que certains clients ne seront pas enclins à divulguer leur capacité de réponse si cela n'a pas été précisé dans les règles d'engagement des tests d'intrusion.

L'IDR est composé de 7 caractéristiques. Il permet de déterminer globalement le niveau de maturité d'un client en se fiant à sa capacité de détection et de réaction. Chaque caractéristique sera énumérée et quantifiée par un entier grâce à une échelle de Likert allant de 1 (niveau le plus faible) à 5 (niveau le plus élevé). Par la suite, le score propre à l'IDR sera obtenu en calculant la moyenne et la médiane des scores de chaque caractéristique. Les scores globaux seront donc interprétés et reflèteront une position propre à la maturité de l'EC. Un environnement peu mature se verra attribuer une note tendant vers 1. Ce sera l'inverse pour un EC très mature.

Tableau 4-8 Détails - Indice de réponse

Caract. 1	**Capacité de détection et de réponse aux techniques de ramassage d'informations actif (*Information Gathering*)**

Tableau 4-8 Détails - Indice de réponse

	1— Nulle (aucun contrôle sur l'information externe) **2— Passable (partiellement conscient des informations concernant l'entreprise, étant disponible de l'externe)** **3— Acceptable (conscient de l'information et revue régulière de ces dernières)** **4— Proactive (contrôle régulier de l'information exposée à l'externe et revue régulière)** **5— Optimale (contrôle régulier et formation des employés aux bonnes pratiques)**
Caract. 2	**Capacité de détection et de réponse aux techniques de relevé d'empreintes (*Foot printing*)**
	1— Nulle (aucun contrôle / pas de préoccupation / pas d'intérêt) 2— Passable (certains équipements sont journalisés, sans revue systématique) 3— Acceptable (tous les journaux équipements et applications sont centralisés) 4— Proactive (acceptable et revue régulière des journaux) 5— Optimale (proactif et alertes automatisées basées sur les modèles de relevés d'empreintes et blacklist temporaire des IP en question)
Caract. 3	**Capacité de détection et de réponse aux scans de vulnérabilités**

Tableau 4-8 Détails - Indice de réponse

	1— Nulle (aucun contrôle / pas de préoccupation / pas d'intérêt) **2— Passable (certains équipements sont journalisés, sans revue systématique)** **3— Acceptable (tous les journaux équipements et applications sont centralisés, personnel formé à la recherche d'entrées spécifiques)** **4— Proactive (acceptable et revue régulière des journaux)** **5— Optimale (proactif et alertes automatisées basées sur les modèles de scans et blacklist temporaire des IP en question)**
Caract. 4	**Capacité de détection et de réponse aux infiltrations / attaques**
	1— Nulle (aucun contrôle / pas de préoccupation / pas d'intérêt) 2— Passable (Présence d'un IDS, journaux non consultés, pas d'alertes) 3— Acceptable (Présence d'un IDS et d'une procédure d'audit régulier, alertes préréglées) 4— Proactive (acceptable, IPS et équipe formée en cas d'intrusions) 5— Optimale (proactive, isolation de l'attaque et traitement post mortem)
Caract. 5	**Capacité de détection et de réponse au rassemblement d'information**

Tableau 4-8 Détails - Indice de réponse

	1— Nulle (aucun contrôle / pas de préoccupation / pas d'intérêt) **2— Passable (les accès sont journalisés)** **3— Acceptable (les accès sont journalisés et revus)** **4— Proactive (acceptable, journalisation d'accès centralisée et alertes en cas d'accès non autorisé)** **5— Optimale (proactif, alertes automatisées basées sur les modèles de relevés d'empreintes et blacklist temporaire des IP en question)**
Caract. 6	**Capacité de détection et de réponse aux transferts non autorisés**
	1— Nulle (aucun contrôle / pas de préoccupation / pas d'intérêt) 2— Passable (les transferts externes de certains équipements sont journalisés) 3— Acceptable (les transferts externes de tous les équipements sont journalisés et revus) 4— Proactive (acceptable et alertes en cas de transferts non autorisés) 5— Optimale (proactif, blocage en temps réel, rapidité d'intervention et enquête)
Caract. 7	**Capacité à mettre à jour et d'éditer les politiques de sécurité de manière dynamique**

Tableau 4-8 Détails - Indice de réponse

	1— Nulle (Aucune politique de sécurité) **2— Passable (Aucune politique, mais noter une présence de contenus documentaires tels que des directives et procédures faisant mention de sécurité des actifs** **3— Acceptable (politique de sécurité à jour)** **4— Proactive (acceptable et changement régulier en fonction des modifications sur l'environnement)** **5— Optimale (proactif, équipe de sécurité et ensemble de directives et procédures de sécurité)**

Exemple :

Entreprise XCA — Environnement ciblé: serveurs web

Tableau 4-9 Maturité sur l'échelle IDR

C1	C2	C3	C4	C5	C6	C7	IDR (MOY)	IDR (Med)
1	5	1	2	3	1	3	3	2

Le tableau ci-dessous permet de représenter les 7 catégories propres à l'IDR. Le score de l'IDR est calculé en additionnant la valeur de chacune des caractéristiques et en faisant une moyenne simple.

4.2 Évaluation du risque

4.2.1 Priorisation et placement

L'étape d'évaluation du risque permet de prioriser les vulnérabilités pour mieux les catégoriser et raffiner les résultats qui permettront d'obtenir un processus de traitement plus ciblé. Pour cela, il est nécessaire de passer à travers plusieurs matrices d'évaluation. Ces dernières vont refléter directement la posture de l'EC en basant l'effort de priorisation sur le total et les ensembles de vulnérabilités.

4.2.1.1 Vulnérabilité

La première matrice est une version classique que l'on peut retrouver dans la classification des risques conventionnels. Elle permet d'afficher les vulnérabilités sur une matrice caractérisant l'impact et la potentialité. Pour cela, chaque vulnérabilité comporte deux caractéristiques propres aux facteurs de potentialité et d'impact définis dans VANSS.

Les codes couleur permettent de représenter les valeurs qualitatives de risque :

- Vert clair : risque imperceptible
- Vert foncé : risque faible
- Orange clair : risque modéré
- Orange foncé : risque élevé
- Rouge : risque très élevé

Les axes de potentialité et d'impact représentent les échelles quantitatives sur lesquelles nous faisons correspondre les vulnérabilités.

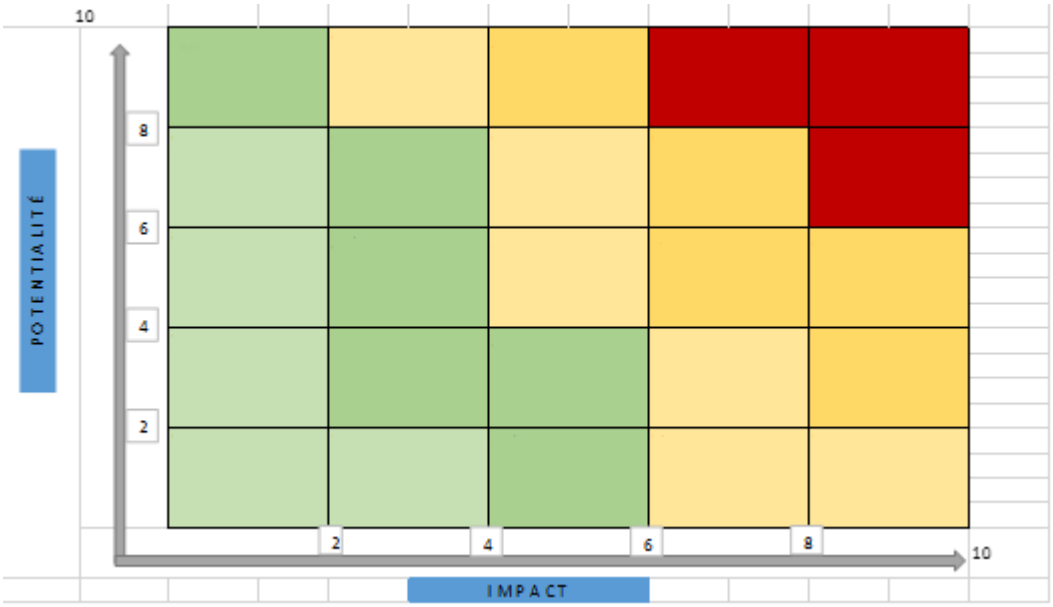

Figure 4-3 Matrice de représentation conventionnelle

Le facteur de potentialité pour une vulnérabilité donnée sera égal à la moyenne des indices du facteur en question.

L'équation suivante permet de traduire le facteur de potentialité sur l'échantillon de vulnérabilité:

$$\overline{x} = \frac{\sum x}{n} \qquad \textbf{(4)}$$

Où $\sum x$ est la somme des indices composant le facteur de potentialité, et n le nombre d'indices dans le facteur. Le facteur d'impact répond exactement à la même équation pour le calcul de la moyenne des scores propres aux facteurs d'impact. Cependant, une importance considérable est à porter sur ce facteur. Dépendamment de la posture de sécurité et de la catégorie d'affaires de l'entreprise dans lequel se trouve l'EC, il est nécessaire de valider les critères de mesure de risque de façon à obtenir une matrice personnalisée et précise.

Le score de potentialité sera calculé par la même méthode que le risque (voir section 4.1.6.4). Nous prendrons seulement en compte les deux facteurs de potentialité ainsi que leurs indices respectifs, comme le montre le tableau ci-dessous.

Tableau 4-10 Facteurs de potentialité

INC	IMO	IOP	IPA	IDE	IEP
FAM (40)				FV (20)	
40				20	
10	10	10	10	10	10
10	4	6	4	4	6
0	0.02	0	0.02	0	0

Le score d'impact sera calculé par la même méthode que le risque (voir section 4.1.6.4). Nous prendrons seulement en compte les deux facteurs d'impact ainsi que leurs indices respectifs, comme le montre le tableau ci-dessous.

Tableau 4-11 Facteurs d'impact

ITP	ISI	IPC	IPI	IPD	IDF	IDR	IIP
FIT (50)					FA (30)		
90					70		
10	10	10	10	50	50	10	10
6	6	10	10	8	10	10	10
0	0	0	0	0.04	0.05	0.05	0

Dès lors, nous obtenons deux valeurs caractérisant la vulnérabilité et son risque.

8	Probabilité :	5.666667	Impact :	8.75

Figure 4-4 Exemple de niveau de risque

Une fois les valeurs respectives des facteurs de potentialité et d'impact obtenues, il est possible de positionner la vulnérabilité en question sur la matrice.

4.2.1.2 Ensemble de vulnérabilité

Les ensembles de vulnérabilités vont être utilisés pour compléter la première matrice selon les règles présentées ci-dessous :

La valeur du facteur de potentialité, pour un ensemble de vulnérabilités données, sera égale à la valeur du facteur de potentialité le plus élevé des vulnérabilités composant l'ensemble.

La valeur du facteur d'impact, pour un ensemble de vulnérabilités données, sera égale à la valeur moyenne des facteurs d'impact de chaque vulnérabilité composant l'ensemble.

Considérons l'exemple suivant où 3 EV sont composées des vulnérabilités suivantes :

Tableau 4-12 Calcul des risques par EV

EV	**Vulnérabilité (Fact Prob / Fact Imp)**	**Facteur Potentialité**	**Facteur Impact**
EV1	V1 (4.5/5.8) V2 (7/5) V3 (5.6/6.5) V4 (4.8/5.8)	7	5.7
EV2	V5 (2.7/5) V6 (3.4/2.3) V7 (2.1/5) V8 (7.2/4.2) V9 (6.1/4.2)	7.2	4.1
EV3	V10 (2.6/5.6) V11 (3/6.2) V12 (5.1/4.3) V13(4.7/4.2)	5.1	5.1

Le tableau ci-dessus permet de représenter la méthode quantitative pour attribuer les valeurs de potentialité et d'impact à un ensemble de vulnérabilité composé de plusieurs vulnérabilités.

Une fois les valeurs des facteurs propres aux EV obtenus, il ne reste qu'à les placer sur la matrice et émettre les observations en accord avec l'étape de priorisation.

Une fois l'étape d'évaluation révolue, il est nécessaire de garder à l'esprit les différents éléments ayant conduit à une priorisation donnée en termes de niveau de risque. Cela permet de conserver le contexte d'évaluation pour ainsi passer au traitement des EV ayant été sélectionnés.

4.3 Traitement

4.3.1 Identification des mesures

Le traitement des vulnérabilités est une étape cruciale dans le cycle d'évaluation des risques. Il permettra de sélectionner les EV et les vulnérabilités associées pour les considérer dans le processus de mise en œuvre des contre-mesures.

Pour le traitement et les recommandations, il est important de mentionner l'utilisation des ressources ci-dessous.

- *Consortium for Internet Security* (CIS) [21]
- Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI)

De plus, grâce à l'orientation d'ITREM vers les normes internationales ISO 27000, la méthodologie permet l'utilisation de l'ISO 27002 et de l'association des EV avec les contrôles propres à la norme. Cela permet de mieux effectuer la liaison entre les différents ensembles de vulnérabilités et les contrôles de sécurité associés.

4.3.2 ISO/IEC 27002:2013 – Technologies de Sécurité

La norme internationale ISO 27002:2013 [22]a pour objet de servir d'outil de référence permettant aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon la norme l'ISO/ CEI 27001 [23] ou de guide pour les organisations mettant en œuvre des mesures de sécurité de l'information largement reconnues. Cette norme a également pour objet d'élaborer des lignes directrices de management de la sécurité de l'information spécifiques aux organisations et aux entreprises, en tenant compte de leur(s) environnement(s) particulier(s) de risques de sécurité de l'information. Elles totalisent 114 contrôles spécifiques et permettent de répondre aux attentes en matière de conformité imposées par ISO 27001 dans le cadre du processus de certification. Ces contrôles vont être directement liés avec les unités de tests d'intrusion.

De plus, pour chaque catégorie de contrôles, il est nécessaire d'orienter les MEGR vers d'autres normes ISO 27000 pour compléter l'étape de traitement avec une norme adaptée ou un guide de contre-mesures.

Des organisations de tous types et de toutes dimensions (incluant le secteur public et le secteur privé, à but lucratif ou non lucratif) collectent, traitent, stockent et transmettent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, au cours de conversations et de présentations).

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles et des fonctions matérielles et logicielles. Ces mesures doivent être spécifiées, mises en œuvre, suivies, réexaminées et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'une organisation. Un SMSI tel que celui spécifié dans l'ISO/ CEI 27001 appréhende les risques de sécurité de l'information de l'organisation dans une vision globale et coordonnée, de manière à mettre en œuvre un ensemble complet de mesures liées à la sécurité de l'information dans le cadre général d'un système de management cohérent.

Nombreux sont les systèmes d'information qui n'ont pas été conçus dans un souci de sécurité au sens de l'ISO 27001 et 27002. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la soutenir à l'aide de moyens de gestion et de procédures adaptées. L'identification des mesures qu'il convient de mettre en place nécessite de procéder à une planification minutieuse et de prêter attention aux détails. Un SMSI efficace requiert l'adhésion de tous les employés de l'organisation. Il peut également nécessiter la participation des actionnaires, des fournisseurs ou d'autres tiers. De même, l'avis et l'intervention de l'ETI et l'EGR, en tant qu'experts externes, se révèlent nécessaires.

De manière plus générale, une sécurité de l'information efficace garantit également à la direction et aux parties tiers que les actifs de l'organisation sont, dans des limites raisonnables, sécurisés et à l'abri des préjudices, et contribuent de ce fait au succès de l'organisation.

4.3.2.1 Requis et exigences en sécurité de l'information

Une organisation doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales:

a) L'appréciation du risque propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux, qui permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel;
b) Les exigences légales, statutaires, règlementaires et contractuelles auxquelles l'organisation et ses partenaires commerciaux, contractants et prestataires de service, doivent répondre ainsi que leur environnement socioculturel;
c) L'ensemble de principes, d'objectifs et d'exigences métier en matière de manipulation, de traitement, stockage, communication et archivage de l'information que l'organisation s'est constituée pour mener à bien ses activités.

Il est nécessaire de confronter les ressources mobilisées par la mise en œuvre des mesures avec les dommages susceptibles de résulter de défaillances de la sécurité en l'absence de ces mesures. Les résultats d'une appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière d'évaluation des risques liés à la sécurité de l'information, ainsi que de mettre en œuvre les mesures identifiées destinées à contrer ces risques.

La norme ISO/IEC 27005:2009, intitulée « Gestion des risques liés à la sécurité de l'information », fournit des lignes directrices de gestion du risque lié à la sécurité de l'information. Cette norme inclut des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque. Cependant, comme mentionnée ci-dessus, ISO 27005 joue beaucoup plus un rôle de guide global permettant par la suite l'appareillement de méthodologies répondant aux exigences normatives. C'est en ce sens que ITREM se calque sur les principes et étapes d'évaluation des risques énumérés à travers ISO 27005.

4.3.2.2 Présentation des contrôles et mesures associées

Selon les cas, il est possible de sélectionner les mesures dans la présente norme (ISO 27002) ou dans d'autres guides, ou encore de spécifier de nouvelles mesures en vue de satisfaire des besoins spécifiques. La sélection des mesures dépend des décisions prises par l'organisation en fonction de ses critères d'acceptation du risque, de ses options de traitement du risque et de son approche de la gestion générale du risque. Il convient également de prendre en considération les lois et règlements nationaux et internationaux concernés. La sélection des mesures de sécurité dépend également de la manière dont les mesures interagissent pour assurer une défense en profondeur. Certaines mesures décrites dans ISO 27002 peuvent être considérées comme des principes directeurs pour le management de la sécurité de l'information et être appliquées à la plupart des organisations. Les mesures et les lignes directrices de mise en œuvre sont disponibles à travers les liens dans le tableau 4-10.

Chaque objectif ou ensemble d'objectifs liés à un contrôle doivent par la suite être quantifiés en termes de temps, coûts et réduction. Cela fait partie de la documentation à produire dans le cadre de la stratégie de sécurité.

Pour sélectionner les effets des contrôles sur le risque et les adapter à l'EC ainsi qu'à la stratégie, veuillez vous référer au tableau de données permettant de prioriser les effets des contrôles en fonction de la situation de l'EC.

Un extrait de ce tableau est disponible en annexe E.

Le tableau permet de classer les contrôles en 5 catégories d'objectifs de réduction de risque :

- Dissuasif : le contrôle permet de réduire l'exposition à la menace.
- Écartement : le contrôle réduit l'impact potentiel.
- Préventif : le contrôle permet de prévenir la vulnérabilité et de ce fait la menace.
- Détection : le contrôle permet l'identification d'un évènement.
- Réactif : le contrôle permet de minimiser les impacts d'une incidente grâce une réaction rapide.

Un contrôle peut être caractérisé par plusieurs objectifs.

Voici les 14 catégories de contrôles présentes dans la norme ISO 27002 et dans d'autres cadres normatifs propres à la sécurité de l'information :

Tableau 4-13 Domaine de sécurité ISO 27002 et normes relatives

1	**Politiques de sécurité de l'information**	**ISO/IEC 27001:2013** **ISO/IEC 27038**
2	Organisation de la sécurité de l'information	ISO/IEC 27003
3	Sécurité des ressources humaines	
4	Gestion des actifs	
5	Contrôle d'accès	
6	Cryptographie	
7	Sécurité physique et environnementale	ISO/IEC TS 30104
8	Sécurité liée à l'exploitation	
9	Sécurité des communications	ISO/IEC 27033
10	Acquisition, développement et maintenance des systèmes d'information	
11	Relations avec les fournisseurs	ISO/IEC 27036
12	Gestion des incidents liés à la sécurité de l'information	ISO/IEC 27035
13	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	ISO/IEC 27031:2011

Tableau 4-13 Domaine de sécurité ISO 27002 et normes relatives

14	**Conformité**	**ISO/IEC 27006:2011** **ISO/IEC 27007:2011**

Les références de traitement ci-dessus prônent l'appareillement des contrôles et contre-mesures avec les EV obtenus lors de l'étape d'évaluation de la méthodologie. Il est donc recommandé d'engager la gouvernance et la gestion de sécurité des actifs sur une base de référence propre à ISO 27001. Pour cela, il est nécessaire de définir la norme et les intervenants, et de décrire quels sont les avantages à maintenir la sécurité de l'information à travers une norme ou un standard reconnu.

4.3.3 **Adaptation aux processus et contrôles clients**

La partie de traitement permet de sélectionner précisément les contre-mesures et correctifs adaptés à la situation du client. Pour cela, il est indispensable, lorsque l'étape de priorisation des vulnérabilités et EV a été effectuée, de passer à travers une revue des équipements et processus liés à la prévention et au traitement des risques sur l'environnement.

CHAPITRE 5 CLASSIFICATION AUTOMATISÉE DES VULNÉRABILITÉS

Une des étapes les plus délicates et potentiellement ardues du processus ITREM, tel que nous l'avons décrit aux chapitres 3 et 4, est celle de la priorisation des vulnérabilités découvertes lors des tests d'intrusion. Cette étape, décrite plus précisément à la section 4.2, nécessite la participation d'experts qui puissent évaluer l'impact des vulnérabilités regroupées par Ensembles de vulnérabilités (EV) en tenant en considération les divers facteurs spécifiques à l'environnement client (EC) et les réalités de l'entreprise.

Afin d'alléger cette tâche par les experts analystes en sécurité informatique, mais aussi dans le but de potentiellement permettre à d'autres non-experts de participer à cette tâche, nous avons tenté dans ce projet d'utiliser des techniques d'intelligence artificielle (IA) afin d'automatiser la détermination des catégories d'impacts des EV. Nous avons utilisé des *Support Vector Machine* (SVM) et la régression logistique pour effectuer notre expérience et essayer d'obtenir un pourcentage élevé de corrélation et de catégorisation correcte.

5.1 Application de l'IA dans la catégorisation de risques

Dans le domaine du génie informatique, et plus particulièrement dans la sécurité de l'information, plusieurs chercheurs se sont intéressés aux méthodes d'intelligence artificielle pour essayer d'apprécier de façon automatisée les risques associés à certaines vulnérabilités dans les systèmes d'information.

Stefan Fenz [24], dans son article, donne en premier lieu une définition sous forme d'ontologie, concernant les vulnérabilités d'un système TI. Cette ontologie permet donc de servir de base pour la construction d'un réseau bayésien. Le but de ce dernier est la détermination de la potentialité des menaces, elles-mêmes définies dans l'ontologie. Pour chaque menace, l'approche de sa solution à travers les réseaux bayésiens permet de lui faire correspondre les vulnérabilités correspondantes. Fenz détermine ses potentialités en utilisant des vecteurs pour chaque vulnérabilité. Il détermine d'ailleurs le poids de chacune à travers un calcul divisant la valeur numérique du vecteur de sévérité par la somme de sévérité de toutes les vulnérabilités propres à la menace. Son approche théorique est pertinente et permet de bien cerner les interactions dans le

modèle de réseau grâce à une ontologie très bien définie. Cependant, ce travail ne restitue pas réellement les problématiques propres aux environnements TI à risque. Il y a beaucoup trop de facteurs sous-jacents à une vulnérabilité pour simplement générer un modèle simpliste sans étude pratique et de simulation du cas. Lui-même le mentionne à la fin de son article.

En ce qui concerne un modèle concret sur la simulation d'un algorithme d'apprentissage automatisé et son implantation, Xiang Chen et Yun Li [25] ont réussi à simuler des attaques par réseau en utilisant des SVM. Ces derniers redéfinissent aussi une ontologie spécifique avant de tester les modèles. Une spécification utile est la personnalisation du modèle d'ontologie autour d'une classification linéaire reposant sur une fonction de classification.

5.2 Approche théorique

L'approche théorique vient donc expliquer en détail quelle est notre problématique, et comment nous allons la résoudre en choisissant de manière pertinente deux algorithmes d'apprentissage supervisé.

Les tests d'intrusion consistent en une méthode dont le but est de simuler une attaque d'un acteur mal intentionné, voire d'un logiciel malveillant. On analyse alors les risques potentiels dus à une mauvaise configuration d'un système, d'un défaut de programmation, ou encore d'une vulnérabilité liée à la solution testée. Lors d'un test d'intrusion, nous nous retrouvons dans la position de l'attaquant potentiel. Le principal but de cette manœuvre est de trouver des vulnérabilités exploitables en vue de proposer un plan de gestion du risque permettant d'améliorer la sécurité d'un système.

Les risques définis sont tous associés avec une ou plusieurs vulnérabilités impactant les systèmes. L'identification des vulnérabilités permet donc d'obtenir un ensemble de failles représentant chacune une menace potentielle et une atteinte aux principes de confidentialité, intégrité et disponibilité.

La gestion des vulnérabilités et des risques associés peut être illustrée par le tableau 4-14 ci-dessous :

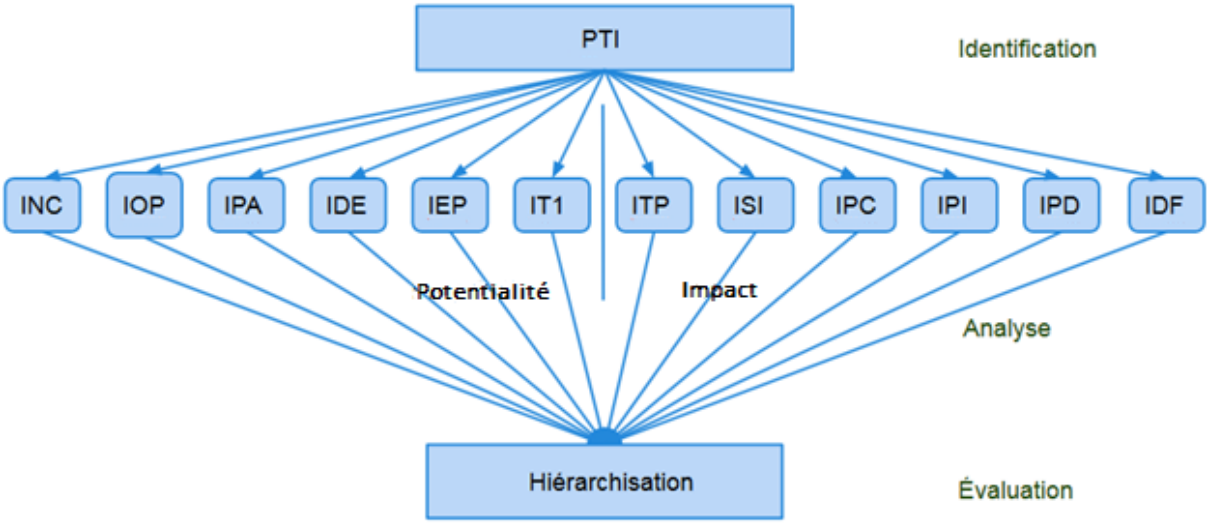

Figure 5-1 Diagramme de représentation de VANSS

L'étape d'identification se résume aux tests d'intrusion. Elle permet de récupérer nos données, à savoir les vulnérabilités.

L'étape d'analyse passe par la quantification des vulnérabilités et de leurs scores de risques. Cela s'effectue .grâce à la mise en place d'indices permettant de sélectionner une valeur numérique sur une échelle de Likert. La combinaison de ces indices permet d'obtenir un score final qui caractérise le risque relatif à la vulnérabilité. Dépendamment du risque et de sa valeur, ce dernier pourra être caractérisé selon le système HML (High, Medium, Low).

Par la suite, l'étape d'évaluation permet de hiérarchiser les vulnérabilités.

Le but est donc de reproduire cette attribution HML de manière automatisée lorsqu'un expert en tests d'intrusion a entré les différentes valeurs par indices.

Les mesures, facteurs et indices propres à ce procédé sont ceux définis plus tôt, dans la section 4.1.4.

INC : Indice de Niveau de compétence

- Expert en recherche de vulnérabilité (10)
- Spécialiste en tests d'intrusion (8)
- Bonne connaissance en programmation, réseau et système (6)
- Utilisateur avancé (4)
- Connaissance partielle de l'informatique (2)
- Pas de connaissance technique en informatique (1)

IMO : Indice de Motivation

IOP : Indice d'opportunité

IPA : Indice de Population d'Agent

Il existe en tout 15 indices pour quantifier une vulnérabilité sur sa posture de risque. Par la suite, faisons une courte exposition théorique des algorithmes que nous allons utiliser.

5.3 Algorithmes de classification utilisés

5.3.1 Support Vector Machines (SVM)

L'émergence des *Support Vector Machines* (SVM) a commencée au début des années 1990, grâce aux efforts de recherches sur l'apprentissage machine par les mathématiciens russes Vladimir Vapnik et Alex Chervonenkis [26]. La première description de l'implantation d'un modèle pouvant être assimilé à un SVM est apparue dans la traduction en Anglais, en 1982, de l'ouvrage de Vapnik «Estimation of Dependences Based on Empirical Data» [27] (édité initialement en russe en 1979).

Le modèle initial à marge maximale a connu des extensions importantes en 1992, qui ont formées le modèle final par l'utilisation de l'astuce du noyau (« kernel trick ») d'Aizeman ,proposé par Boser, Guyon & Vapnik [28], et présenté dans un article à la conférence COLT 92. Finalement, les SVM sous leur forme actuelle ont été introduits en 1995 par V.Vapnik & C.Cortes après l'introduction du «soft margin». Les SVM peuvent être utilisés pour résoudre des problèmes de discrimination, c'est-à-dire décider à quelle classe appartient un échantillon, ou de régression, c'est-à-dire prédire la valeur numérique d'une variable; on parle alors de SVR.

De manière spécifique les SVM permettent d'obtenir un séparateur à marge maximale, une frontière de décision avec la plus grande distance possible entre les points d'apprentissage. Les SVM créent des hyperplans (séparateurs linéaires), et sont aussi capables de projeter les données dans un espace de dimension plus grande en utilisant l'astuce du noyau. Ci-dessous les principales caractéristiques des SVM :

- Le séparateur doit correspondre avec un hyperplan, défini par$\{x: f(x) = w^T x + w_0 = 0\}$.
  - *w* vecteur de poids;
  - *x* vecteur d'entrée;
- La règle de classification $G(x) = (w^T x + w_0) = 0$
  - Avec une optimisation lorsque w et w_0 remplissent ces conditions
- Pour les données séparables : $y_i f(x_i) > 0, \forall i$.

Le but est donc de chercher l'hyperplan ou la droite séparatrice à marge maximale. Afin d'obtenir l'hyperplan optimisé tout en utilisant l'astuce du noyau, on remplace W par la valeur optimale W* :

$$h(x) = \sum_{k=1}^{p} \alpha_j^* y_j K\left(x^T x_j\right) + w_0 \quad \textbf{(5)}$$

Avec :

- $h(x)$ représentant l'équation de l'hyperplan;
- α_j^* représentant les multiplicateurs optimaux (Lagrange);
- K($x^T x_j$) représentant la fonction noyau ;
- w_0 représentant le vecteur support optimal.

Par la suite il suffit de remplacer $x^T\, x_j$ par $f(x_i)^T f(x_j)$. Cela permet d'obtenir un noyau optimal $K(x_i, x_j)$.

5.3.2 **Régression logistique**

La régression logistique se définit comme étant une technique permettant d'ajuster une surface de régression à des données lorsque la variable dépendante est dichotomique. Cette technique est utilisée pour des études ayant pour but de vérifier si des variables indépendantes peuvent prédire une variable dépendante dichotomique. Contrairement à la régression multiple et l'analyse discriminante, cette technique n'exige pas une distribution normale des prédicteurs, ni l'homogénéité des variances. Différents types de régression logistique existent, possédant chacun leur procédé statistique et conduisant à l'élaboration de différents modèles théoriques.

L'objectif dans notre cas est la potentialité d'appartenance à une des trois classes de risque, soit une classe <<k>>. Nous allons donc exposer en détails le modèle multinomial :

$$\pi_k(\omega) = P[Y(\omega)] = y_k/X(\omega) \qquad \textbf{(6)}$$

Avec :

- $\pi_k(\omega)$ représentant les variables prédictives;

- $Y(\omega)$ représentant la variable à prédire;

sous la contrainte$\sum_k^1 \pi_k\,(\omega) = 1$.

La détermination de la vraisemblance passe par une généralisation du modèle binomial :

$$L = \prod \omega[\,\pi_1(\omega)]^{y_1(\omega)} \times \ldots \times [\pi_k(\omega)]^{y_k(\omega)} \qquad \textbf{(7)}$$

avec $y_k(\omega) = 1\ ssi\ Y(\omega) = y_k$.

La modélisation repose sur les rapports de potentialités en prenant une modalité comme référence et en exprimant LOGIT (fonction de linéarisation) par rapport à cette dernière. La potentialité d'appartenance à la *k*-éme catégorie est déduite des autres :

$$\pi_K(\omega) = 1 - \sum_{k=1}^{K-1} \pi_k\,(\omega) \qquad \textbf{(8)}$$

L'équation LOGIT s'écrit sous la forme :

$$LOGIT_k(\omega) = \ln[\frac{\pi_k(\omega)}{\pi_K(\omega)}] = a_{0,k} + a_{1,k}X_1(\omega) + \cdots + a_{J,k}X_J(\omega) \qquad \textbf{(9)}$$

Avec :

- $a_{0,k}$ représentant les coefficients de régression

On peut en déduire les potentialités d'appartenance au groupe :

$$\pi_k(\omega) = \frac{\exp^{LOGIT_k(\omega)}}{1 + \sum_{k=1}^{K-1} \exp^{LOGIT_k(\omega)}} \qquad \textbf{(10)}$$

C’est exactement ce que nous désirons achever à travers l’apprentissage supervisé, sur notre base de score de risque.

5.4 Approche pratique

Dans la partie précédente, nous avons détaillé les deux algorithmes que nous allons comparer : la régression logistique et les SVM. Dans cette partie, nous allons détailler la mise en œuvre pratique de cette comparaison.

5.4.1 **Jeu de données**

Dans le domaine de l’apprentissage automatisé, un des points cruciaux est d’avoir un jeu de données réaliste ou suffisamment réaliste afin de pouvoir entrainer correctement le modèle choisi. Or, notre projet s’appuyant sur ITREM, il n’existe pas encore de jeu de données assez volumineux adapté à ce problème.

Pour remédier à cela, nous avons décidé de collecter un certain nombre de vulnérabilités (500), de spécifier les différentes variables d’entrées présentées ci-dessous et enfin de les étiqueter suivant l’échelle HML (high, medium, low). Étant donné notre expérience professionnelle, nous pouvons considérer que les données ont été étiquetées par un expert, ce qui se fait en pratique en intelligence artificielle. En effet, à l’heure actuelle, la seule façon de déterminer le niveau de risque d’une vulnérabilité est de demander à un expert en sécurité informatique qui, selon son expérience, la classifiera dans telle ou telle catégorie.

Le travail de labélisation étant effectué, nous obtenons un échantillon de 500 vulnérabilités. Voici un extrait de notre fichier de données :

V1,3,2,5,2,3,5,4,6,1,2,1,1,2,6,0,Medium

V2,1,2,5,2,5,8,5,2,1,2,1,1,2,8,0,High

V3,5,7,9,2,1,8,5,2,8,2,8,6,8,8,0,High

V4,3,2,5,4,1,8,1,4,1,2,7,6,2,5,0,Medium

Cet extrait représente les paramètres de vulnérabilité comme suit :

- V1, représentant la référence de la vulnérabilité
- 3,2,5,2,3,5,4,6,1,2,1,1,2,6,0 score de potentialité et d'impact
- Medium, représentant le risque qualitatif

Voyons maintenant comment cela est implémenté techniquement.

5.4.2 Implantation

L'implantation de nos deux modèles a été réalisée en Python3 à l'aide des bibliothèques LibSVM et Scikit-l learn.

`LibSVM` [29] est une librairie externe, développée en C++, de la National Taiwan University et qui propose de nombreuses interfaces : Python, Matlab, Weka, etc. C'est une des implantations des SVM les plus performantes à l'heure actuelle et c'est donc pour cela qu'elle est très répandue.

`Scikit-learn` est une librairie Python qui propose un nombre important d'algorithmes d'apprentissages, qu'ils soient de classification, de régression, de mise en grappe (« clustering ») ou encore de réduction de dimension. Nous avons donc choisi de l'utiliser dans la régression logistique en raison notamment de l'importante documentation qui est proposée sur le site internet de Scikit [30]. Enfin, cette librairie semble réputée puisqu'elle est financée par Google et l'INRIA et utilisée par Spotify ou encore Evernote.

Dans un premier temps, nous avons transformé nos données CSV en deux listes pythons : une pour les entrées et une pour les labels HML. Ces derniers ont été convertis en valeur numérique (1, 2, 3), car l'implantation de la régression logistique utilisée ne permet pas l'utilisation de label sous forme de texte.

L'entrainement et le test du SVM sont présentés dans le code ci-dessous, où sont définis les labels et les variables d'entrées. On notera que nous avons choisi d'entrainer le modèle sur deux tiers des données et de la valider sur le tiers restant. Ainsi la variable *train* est égale à 350.

```
#Entrainement du svm
prob = svm_problem(y[:train],x[:train])
param = svm_parameter(« -s 0 – t 3 – b 1')
#C-SVM et kernel polynomial
```

```
# -b 1 Permet l'estimation probabiliste (% de chance pour que ça soit dans
chaque classe -> confiance du résultat)
m = svm_train(prob, param)

#Validation
p_label, p_acc, p_val = svm_predict(y[train:], x[train:], m)
```

L'entrainement et le test de la régression logistique sont présentés dans le code ci-dessus.

```
#Entrainement
model = LogisticRegression(C=3, penalty='l1', tol=1e-6)
model.fit(x[:train],y[:train])
#Validation
print("LogisticRegressionCV Score : "+str(model.score(x[train:],y[train:])))
```

5.5 Résultats

5.5.1 Score

Dans la figure 5-2 Comparaison des scores, est représenté le score de nos deux algorithmes : Régression logistique et SVM. À titre indicatif, nous avons aussi inséré l'algorithme Decision Tree dans notre comparaison. On remarque que les SVM sont donc plus performants de 5 % comparé aux deux autres méthodes. Cela s'explique en partie par le fait que les SVM sont très robustes, car de par leur construction, l'hyperplan séparateur a une marche maximale par rapport aux vecteurs de support.

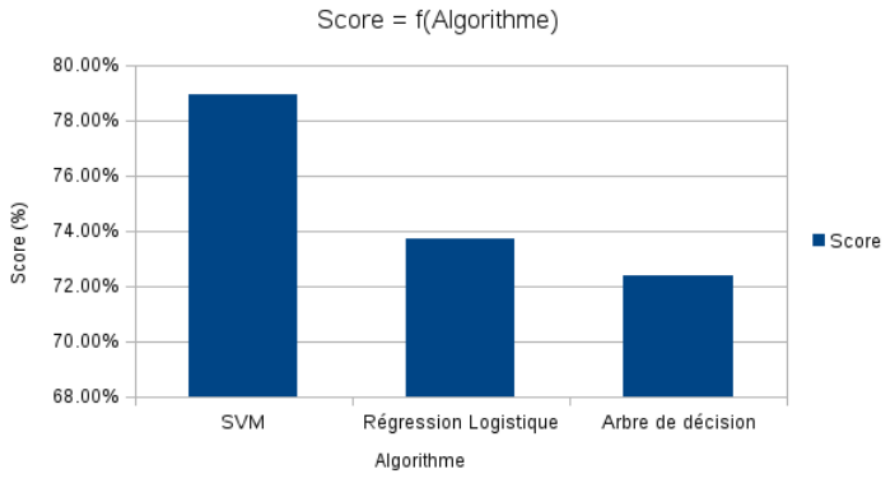

Figure 5-2 Comparaison des scores

5.5.2 Choix des paramètres

En réalité, les scores présentés dans la section précédente sont ceux qui ont été obtenus après la phase d'affinage des paramètres. En effet, dans tous les modèles de Machine Learning, il faut adapter les paramètres à l'ensemble de validation, à défaut de celui d'entrainement, afin d'avoir de meilleurs résultats sur l'ensemble de tests. Il s'avère que dans notre cas, l'affinage sur le modèle d'entrainement permet de meilleurs résultats sur l'ensemble de validation, étant donné que nous n'avions pas assez de données pour avoir aussi un ensemble de tests.

Dans le cas de la régression logistique, les deux paramètres importants sont la norme utilisée, ici L1 ou L2, et la valeur de C, qui intervient dans la fonction de minimisation. Nous avons calculé les scores pour des valeurs de C de 1 à 10 avec une norme L1 ou une norme L2. Il s'avère que l'augmentation sur le score d'entrainement se répercute bien sur le score de validation. Les résultats sur l'ensemble de validation sont visibles à travers la figure 5-3.

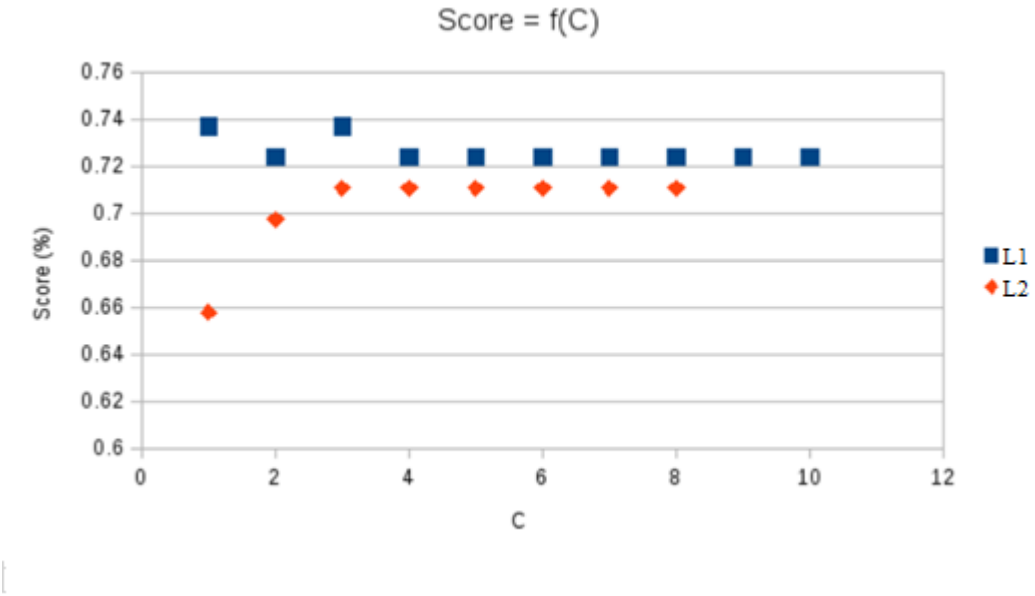

Figure 5-3 Score de tests pour différente valeur de C

On y observe que mis à part le point (L2, $C = 1$), les autres points sont vraiment très proches. Ainsi la norme et le paramètre C n'ont pas une grande influence sur le résultat final, généralement pas plus de deux points sur une échelle de cent. Néanmoins, nous avons choisi le

meilleur couple de points, c'est-à-dire la norme L1 et C égaux à 3. On notera que la norme L1 et C=1 conduisent au même résultat.

Dans le cas du SVM, le principal paramètre est le choix du noyau. En effet, lorsque les données ne sont pas linéairement séparables, il faut augmenter la dimension de l'espace des données afin de trouver un bon hyperplan séparateur. Généralement, dans la plupart des librairies et logiciels de datamining, quatre noyaux sont proposés par défaut : Linéaire, Polynomial, Radial Basis function[1] et Sigmoid[2]. Les résultats sont présentés dans la figure 5-4. Dans le cas de ce problème, c'est donc le noyau polynomial qui est le plus adapté puisqu'il permet d'avoir près de 80% de résultats positifs contre à peine 60% pour le noyau sigmoïde.

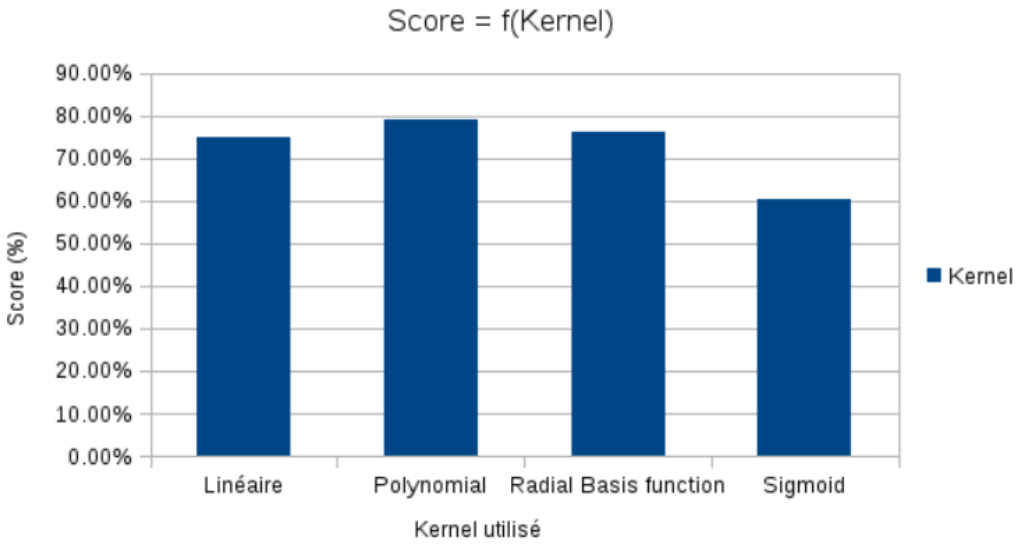

Figure 5-4 Score de tests pour différents noyaux (« kernels »)

[1]Fonction pour laquelle $\forall x \in D, \phi(x) = \phi(\| x \|)$

[2]Fonction définie telle que $\forall x \in D, f(x) = \frac{1}{1+e^{-\lambda x}}$

5.5.3 **Temps d'exécution**

En dehors du pourcentage de vulnérabilités bien classées, la performance d'un algorithme doit aussi être évaluée en termes de temps d'exécution. En effet, l'apprentissage se fait idéalement sur un très grand nombre d'échantillons et il est donc souhaitable que le temps de calcul n'explose pas. Sur la figure 5-5 sont représentés les différents temps d'exécution. Ce sont des moyennes obtenues après 10 exécutions successives. Ce temps de calcul ne prend bien entendu pas compte de l'analyse au préalable des données, mais seulement du temps nécessaire à l'apprentissage et à la validation du modèle.

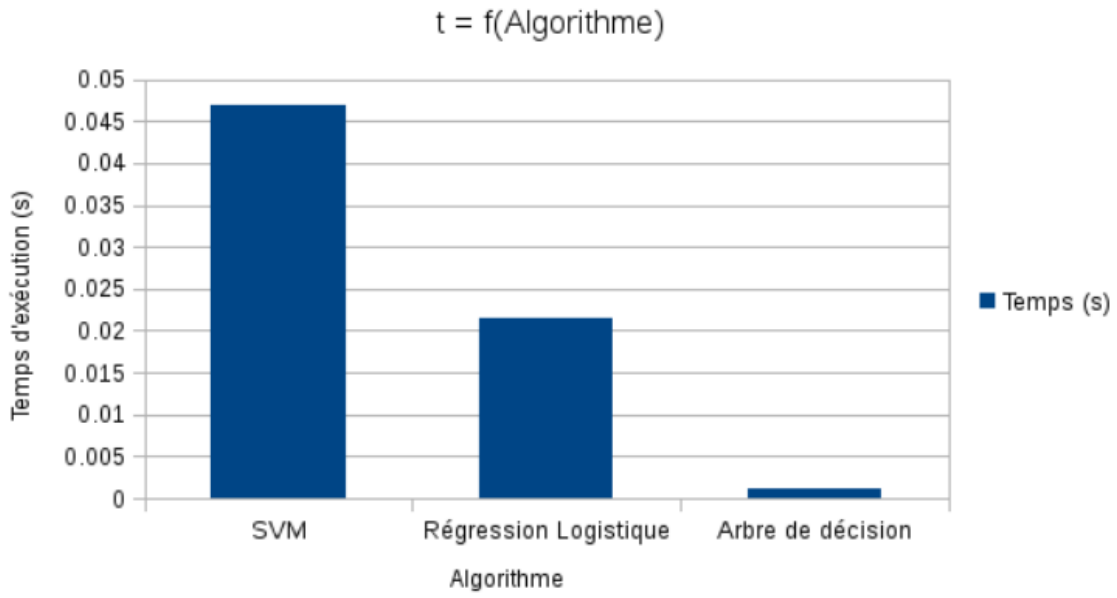

Figure 5-5 Temps d'exécution (apprentissage & validation)

On notera qu'ils sont ici très faibles, car nous avons un nombre très limité de données, soit trois cents.

Ainsi, on retrouve l'inverse de la hiérarchie des scores. L'algorithme donnant les meilleurs résultats, SVM, est aussi le plus lent. Trois ordres de grandeur séparent l'algorithme SVM de l'algorithme Decision Tree. Cependant, même dans le cas de plusieurs milliers de données, le temps d'exécution du SVM devrait rester raisonnable.

Dans le cas d'un système assez sensible, classifiant des vulnérabilités, et sachant que l'apprentissage n'est effectué qu'une fois, avant la livraison finale du logiciel de classification, il ne nous paraît pas pertinent de considérer cette mesure de façon très importante.

5.6 Discussion

D'une part, le but premier de cet outil d'aide à la décision était de montrer qu'il est possible de remplacer une tache particulière d'un expert en sécurité par un algorithme d'apprentissage machine supervisé, en ce qui a trait à l'évaluation sur une échelle de risque des vulnérabilités. Les résultats que nous avons obtenus ne sont, au premier abord, pas satisfaisants afin de remplir pleinement ce but. En effet, nous avons obtenu au mieux 78% de bons résultats. Cela peut paraître correct, mais, quand il s'agit d'évaluer un risque pour une entreprise qui se chiffre ensuite en un coût, il n'est pas possible d'accepter une telle marge d'erreur.

Afin de remédier à cela, nous avons décidé d'utiliser l'algorithme Support Vector Machine en mode probabiliste. Ainsi, la sortie n'est plus un choix dans l'ensemble des sorties possibles, mais la potentialité correspondante à tel ou tel choix. Ainsi, une sortie pourrait être 80% High, 15% Medium et 5% Low. Dans ce cas, le non-expert utilisant l'algorithme sélectionnera sans trop de difficultés le choix High. En revanche, si la sortie est 40% High, 40% Medium et 20% Low, l'utilisateur saura que la sortie n'est pas certaine et il pourra dans ce cas aller se renseigner auprès d'un expert lorsque cela se produit.

Ainsi, si cet algorithme n'est pas capable de remplacer entièrement un expert, il est un bon aide à la décision et réduira l'importance d'avoir un expert dédié à cette tâche. Ce dernier interviendra toujours en cas de besoin, mais pourra le reste du temps se consacrer à des tâches plus difficiles.

D'autre part, nous avons réalisé l'apprentissage sur un nombre très restreint d'échantillons, à savoir 500. En effet, il est très long d'annoter chaque vulnérabilité, ce qui justifie d'autant plus l'usage de l'intelligence artificielle. En outre, nous avons exploré seulement deux (voire trois)

algorithmes de régression, même si les SVM sont actuellement un des algorithmes de régression les plus performants.

CHAPITRE 6 ÉTUDE DE CAS

6.1 Contexte de l'étude

L'étude de cas actuelle recense le cheminement et les résultats propres à la première implantation de la méthodologie ITREM dans un environnent réel et contenant des actifs critiques. Nous avions donc choisi une entreprise dans le domaine de la finance et de l'investissement privé.

De façon à préserver l'anonymat de l'entreprise ciblée, nous l'appellerons FINTRADE.

FINTRADE est une entreprise de gestion de patrimoine canadienne ayant plus de 1000 employés. Elle dispose de plusieurs actifs critiques dont des données bancaires, des brevets, des algorithmes d'ordres boursiers automatisés ainsi que des données relatives à ses employés.

Les ressources de FINTRADE, spécialisées en sécurité de l'information, avaient fait part de leur incapacité à interpréter et évaluer les risques découlant des exercices de tests d'intrusions. Ces tests, ciblant la totalité de l'environnement numérique de l'entreprise, avaient été effectués plusieurs mois auparavant et avaient généré des rapports très volumineux en termes de vulnérabilités. La mission était donc de fournir à FINTRADE, par le biais d'un mandat de consultation, une orientation et une prise de positionnement quant au traitement des vulnérabilités et risques associés.

6.2 Processus de tests d'intrusion (PTI)

6.2.1 Identification des risques

Dans le but de fournir à ses clients l'une des meilleures qualités de service en tests de pénétration, les experts en sécurité d'OKIOK se sont appuyés sur les bases de vulnérabilités et de connaissances, incluant les exploits et techniques d'attaque les plus récents. Cette méthode, utilisée pour tous les tests de pénétration qu'OKIOK réalise pour ses clients, s'appuie sur diverses normes de l'industrie en termes de tests de pénétration, et en particulier OSSTMM [31] et l'OWASP [32].

Avec la méthodologie ITREM, nous croyons que les bases d'attaque et d'exploit peuvent être utilisées comme une source d'identification d'une grande partie des failles de sécurité. Ainsi, nous

avons commencé à partir de cette source, et nous y avons ajouté les résultats des tests d'intrusion afin d'articuler notre processus méthodologique. Pour rappel, l'environnement numérique de FINTRADE a été soumis à plusieurs tests d'intrusion et ces résultats ont permis de servir d'intrants, comme prévu par le processus d'identification des risques.

6.2.2 **Portée de la mission**

Cette section décrit la portée des activités de tests d'intrusion. L'évaluation des risques fut fondée sur les rapports générés par les différentes activités de tests d'intrusion ci-dessous. Nous avons donc défini notre modèle d'évaluation des risques en nous appuyant sur les données factuelles obtenues grâce à chaque activité de tests. Chaque vulnérabilité, dans les rapports de tests d'intrusion, fut considérée comme un risque d'atteinte à la confidentialité, disponibilité et intégrité des données de FINTRADE, comportant le niveau approprié d'impact et de potentialité. Suite à une entente commune avec le client, nous avons considéré que cette approche technique ainsi que la portée de cette mission devait faire l'objet d'un appareillement normatif.

À cet effet, nous avons déterminé quelles étaient les obligations en termes de normes et de références normatives propres à la sécurité de l'information. La norme choisie fut la NIST SP800-30 « Guide for conducting Risk Assessment » [33], avec la sous-catégorie de la norme : Tiers 3, correspondant à un risque tactique (technique) ; les risques tactiques sont le dernier niveau de détails observés par la norme du NIST.

6.2.3 **Domaines de tests d'intrusion inclus dans ITREM**

• Activité 1 (T1) : Escalade de privilège à partir d'un poste de travail employé

• Activité 2 (T2) : Station de travail fermée et verrouillée

• Activité 3 (T3) : Test interne

• Activité 4 (T4) : Test d'ingénierie sociale

• Activité 5 (T5) : Test de sécurité physique

• Activité 6 (T6) : Test de sécurité de la solution de virtualisation

• Activité 7 (T7) : Test de sécurité de la solution de sauvegarde

• Activité 8 (T8) : Tests de sécurité réseau

Ci-dessous, la figure 6-1 résume la répartition des vulnérabilités en catégories d'activité.

Nombre total de vulnérabilités identifiées : 23

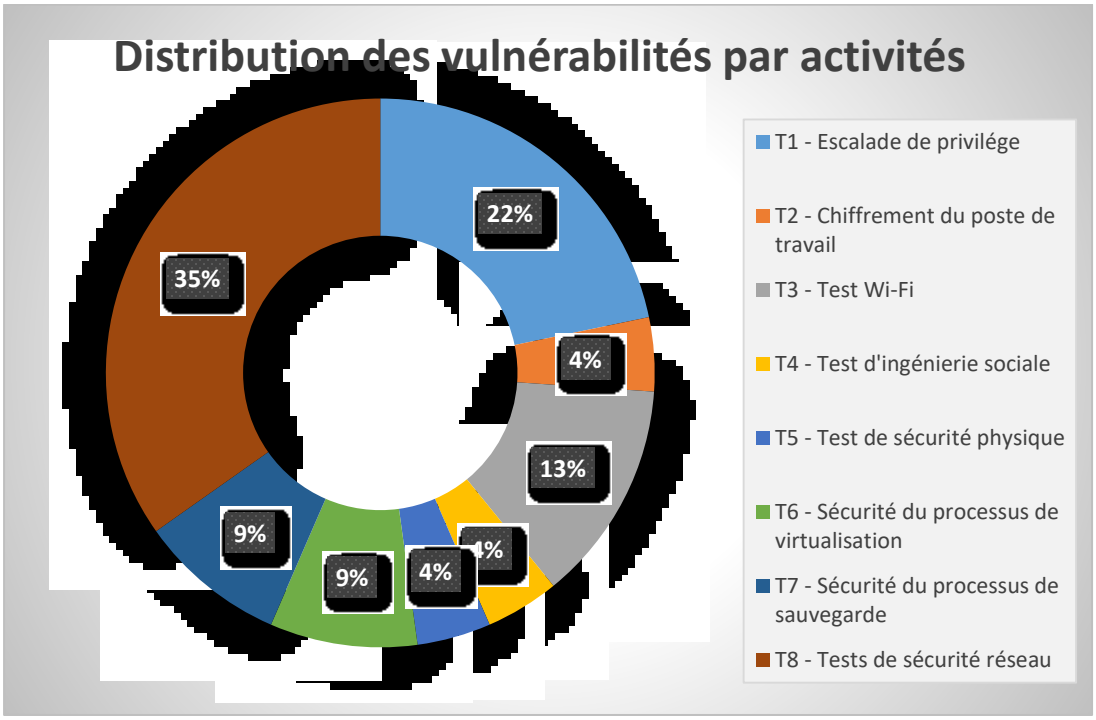

Figure 6-1 Distribution des vulnérabilités en fonction des activités du PTI

6.3 Processus d'appréciation du contexte (PAC)

6.3.1 Contexte client

FINTRADE a choisi cette approche d'évaluation des risques dans le but de structurer les résultats des tests d'intrusion et les risques relatifs. Un des objectifs fut aussi d'établir les priorités de traitement et d'obtenir certains indicateurs de sécurité. Il était essentiel que la méthode fournisse des mesures de contrôle adaptatives afin de suivre les pratiques de gestion du risque déjà mises en œuvre par FINTRADE. Le référentiel normatif choisi conjointement par les équipes de

FINTRADE et par OKIOK, est le NIST SP800-30 [33] pour l'évaluation des risques et contrôles, et le NIST SP800-53 pour l'identification.

Pour intégrer le processus d'évaluation des risques dans l'ensemble de l'organisation et afin de traiter plus efficacement les préoccupations d'affaires, une approche à trois niveaux fut envisagée pour la réponse aux risques:

- Niveau 1 — Organisationnel;
- Niveau 2 — Mission et processus d'affaires;
- Niveau 3 — Système d'information.

Le processus d'évaluation des risques a été effectué sur un seul niveau (niveau 3) avec l'objectif global d'amélioration continue pour les activités connexes reliées à la gestion du risque dans l'environnement. De plus, cela a permis de conserver une efficacité inter et intra-niveau en ce qui a trait à la communication entre toutes les parties prenantes ayant un intérêt commun à la réussite de l'entreprise et au succès de la mission organisationnelle. Grâce à cet exercice de gestion, nous nous sommes concentrés principalement sur le niveau 3 (niveau des systèmes d'information), car nous nous sommes appuyées sur les intrants et parties techniques liés aux tests d'intrusion.

Les scénarios de risque liés à des violations de données ont été discutés et définis avec FINTRADE pour faciliter la classification des risques. La catégorie ici présentée permet de faciliter la classification des risques techniques tout en faisant référence à notre cadre normatif (NIST SP800-53 et SP800-30)

Catégorie de fuite de données (dommage, les fuites, et l'accès) identifiées :

- [0603] Un support portable contenant des données sensibles est perdu ou divulgué.
- [0604] Perte de données sensibles ou divulgation par attaque logique.
- [0605] Les supports de sauvegarde sont perdus ou les sauvegardes ne sont pas contrôlées régulièrement.
- [0606] L'information sensible est accidentellement divulguée en raison des directives de manipulation n'ayant pas été suivies.
- [0607] Les données sont modifiées de manière intentionnelle.

- [0608] Les informations sensibles sont communiquées par courrier électronique ou les médias sociaux.
- [0609] L'information sensible est découverte en raison de l'inefficacité conservant/archivant/éliminant de l'information.

Ces catégories nous ont aidées à constituer le processus de classification des vulnérabilités.

6.3.2 **Formulation des objectifs**

Le département de la sécurité de l'information d'affaires de FINTRADE a déterminé que les précédents exercices de tests d'intrusion ont généré trop de recommandations. Par conséquent, ils ont déterminé qu'une évaluation des risques basée sur les tests de pénétration propres à l'environnement numérique de FINTRADE représenterait une valeur ajoutée. L'objectif principal de cette mission était donc d'effectuer une évaluation des risques des systèmes d'information appartenant à FINTRADE, basée sur les résultats et vulnérabilités rapportés par l'équipe de tests d'intrusion. L'objectif spécifique de ce rapport fut de fournir un guide sur le processus de priorisation des traitements et les indicateurs d'exposition, à la suite de l'évaluation des risques.

6.3.3 **Revue des tâches**

Les tâches principales du projet furent ordonnancées selon l'ordre suivant :

- Contexte d'évaluation des risques FINTRADE
- Identification des risques
- Analyse des risques
- Évaluation des risques
- Stratégie de traitement des risques
- Indicateurs de sécurité

6.4 Processus d'évaluation de risques (PER)

6.4.1 Introduction des risques

6.4.1.1 Risques résiduels actuels (A/CA)

Ils furent définis en tenant compte des contrôles présents dans l'environnement actuel, ce que nous désignons avec l'acronyme A/CA. Ils ont été une réflexion des vulnérabilités et des résultats de l'analyse des risques, correspondant à ceux évalués tout au long des activités de tests d'intrusion.

6.4.1.2 Risques résiduels avec contrôles recommandés (A/CR)

Ils furent redéfinis et évalués selon les contrôles de traitement les plus adaptés et recommandés, situation désignée par A/CR, et ont été basées sur une approche d'atténuation des risques en appliquant des contrôles connexes et/ou contre-mesures. Plusieurs rencontres préalables avec l'équipe d'évaluation des risques de FINTRADE ont dû être organisées pour évaluer les niveaux se rapportant aux traitements des risques. Suite à un commun accord sur les traitements effectifs, nous avons pu comparer et évaluer le niveau résiduel de l'ensemble des risques identifiés au départ.

6.4.2 Analyse des risques

L'approche utilisée pour quantifier les risques liés à chaque vulnérabilité fut basée sur deux mesures, soit l'impact et la potentialité.

6.4.2.1 Échelles de calculs des risques

6.4.2.1.1 Impact

Afin de pouvoir évaluer le niveau de sévérité des vulnérabilités identifiées, nous avons fait référence au système d'évaluation d'impacts des vulnérabilités *Common Vulnerability Scoring System* version 2 (CVSSv2). Ce système d'évaluation a permis de rapidement évaluer les vulnérabilités identifiées pour prioriser la mise en place de correctifs.

Le système CVSS est composé de trois groupes de mesures :

- mesures de base;
- mesures temporelles;
- mesures environnementales.

La mesure de base représente le caractère intrinsèque et fondamental de sévérité des vulnérabilités, et ne change pas dans le temps ou en fonction de l'environnement d'utilisation des systèmes. C'est cette mesure que nous avons évalué lors de l'analyse d'impact des vulnérabilités.

Les mesures temporelles et environnementales représentent des caractéristiques qui sont particulières à l'environnement et aux conditions d'utilisation des systèmes et sont mieux évaluées par FINTRADE.

De plus, les tests d'intrusion ayant été évalués à travers CVSS, la mesure d'impact de VANSS n'a pas été utilisée lors de l'exercice de quantification d'impact.

Le score CVSS de base est une valeur sans unité entre 0 et 10. Afin de pouvoir adapter les scores CVSS à l'échelle d'impact du NIST, nous avons suivi l'approche du NIST sur la classification en classant les scores d'impact sur cinq sous-ensembles :

Tableau 6-1 Échelle d'impact pour l'étude de cas FINTRADE

Score	Impact
0 — 0,5	Imperceptible
0,5 – 2	Faible
2 — 6,9	Modéré
7 — 9	Élevé
9 — 10	Très élevé

6.4.2.1.2 Potentialité

Afin d'évaluer le niveau de potentialité associé à des vulnérabilités identifiées, nous avons employé la méthode VANSS. Bien que VANSS soit composé de deux mesures, impact et potentialité, nous avons utilisé uniquement celle liée à la potentialité. Comme CVSS a été utilisé pour analyser l'impact pendant les tests de pénétration, nous avons évalué la potentialité grâce à la mesure de VANSS de façon à apporter les niveaux appropriés.

La mesure de potentialité fut composée par deux facteurs et six indices, comme indiqué ci-dessous et décrit au chapitre 4 (Section 4.1.4.2) :

- Facteur Agent de Menace (FAM) :
    - Indice de compétence (INC)
    - Indice de motivation (IMO)
    - Indice d'opportunité (IOP)
    - Indice de population de l'agent (IPA)
- Facteur de Vulnérabilité (FV) :
    - Indice découverte (IDE)
    - Indice d'exploitation (IEP)

Ces indices sont composés de plusieurs paliers qui constituent la valeur quantitative.

Tel que décrit au chapitre 4, VANSS utilise à la base une échelle numérique entre 0 et 10 pour évaluer la potentialité de matérialisation d'une menace. Afin de pouvoir adapter les scores de VANSS à l'échelle de potentialité du NIST, tel qu'exigé par le client, nous avons suivi l'approche du NIST sur la classification en classant les scores de potentialité sur cinq (5) sous-ensemble :

Tableau 6-2 Échelle de potentialité pour l'étude de cas FINTRADE

Score	Potentialité
0 — 0,5	Imperceptible

Tableau 6-2 Échelle de potentialité pour l'étude de cas FINTRADE

0,5 – 2	Faible
2 — 6,9	Modérée
7 — 9	Élevée
9 — 10	Très élevée

L'une des valeurs ajoutées de VANSS repose dans le facteur de pondération qui peut être attribué à n'importe quel indice. Cela a permis une priorisation contextuelle basée sur la quantification des scores de potentialité propres aux résultats des activités de tests d'intrusion de FINTRADE.

6.4.2.1.3 Classification des vulnérabilités

VANSS introduit la notion d'Ensemble de Vulnérabilité (EV) de façon à fournir un plus haut niveau de classification. L'objectif principal fut de pouvoir classer chacune des vulnérabilités dans un ensemble. Chaque ensemble est simplement une référence à un contrôle de sécurité. De cette façon, les ensembles de vulnérabilités, relatifs à FINTRADE, ont pu être traités grâce à des contrôles communs et ainsi permettre une convergence plus rapide et optimisée vers les cibles de maturité, en matière de sécurité.

La priorité des contrôles relatifs au référentiel du NIST a été établie ainsi :

Tableau 6-3 Codes de priorité du cadre référentiel NIST SP800-30

Code de priorité	Séquencement	Action
Code de priorité 1 (P1)	Premier	Implémenter les contrôles de sécurité P1 en premier.

Tableau 6-3 Codes de priorité du cadre référentiel NIST SP800-30

Code de priorité 2 (P2)	Suivant	Implémenter les contrôles de sécurité P2 après P1.
Code de priorité 3 (P3)	Dernier	Implémenter les contrôles de sécurité P3 après P2.
Priorité non déterminée (P0)	À déterminer	Les contrôles de sécurité ne sont pas sélectionnés.

Dans cette section sont identifiés tous les ensembles de vulnérabilités recensés dans les activités d'intrusions/tests de système.

Tableau 6-4 EV et représentation de leur catégorie de contrôle

Ensembles de vulnérabilités	Catégorie de contrôle
EV 1	Configuration
EV 2	Gestion de l'authentification
EV 3	Mesures cryptographiques
EV 4	Intrusion physique
EV 5	Contrôles d'accès, permission et privilèges
EV 6	Erreurs de gestion
EV 7	Fonctionnalité de sécurité
EV 8	Manipulation des supports de données

La figure suivante, 6-2, est utilisée pour répertorier les ensembles de vulnérabilités ainsi que les mesures de potentialité et d'impact par vulnérabilité identifiée. La majorité des valeurs qualitatives et quantitatives ont été classées comme modérées en raison de la norme NIST SP800-R30 concernant l'échelle de classification. La matrice de représentation du risque, en suivant l'échelle citée plus haut, comporte un segment de classification alloué pour le niveau modéré situé entre 2 et 6,9 sur 10 pour chaque mesure, ce qui a eu pour effet de couvrir une grande partie de la matrice de risque. Cela pourrait porter à confusion quant à l'attribution du qualificatif de risque, cependant après une revue détaillée du fonctionnement de la matrice, FINTRADE fut d'accord pour utiliser le système de score tel quel.

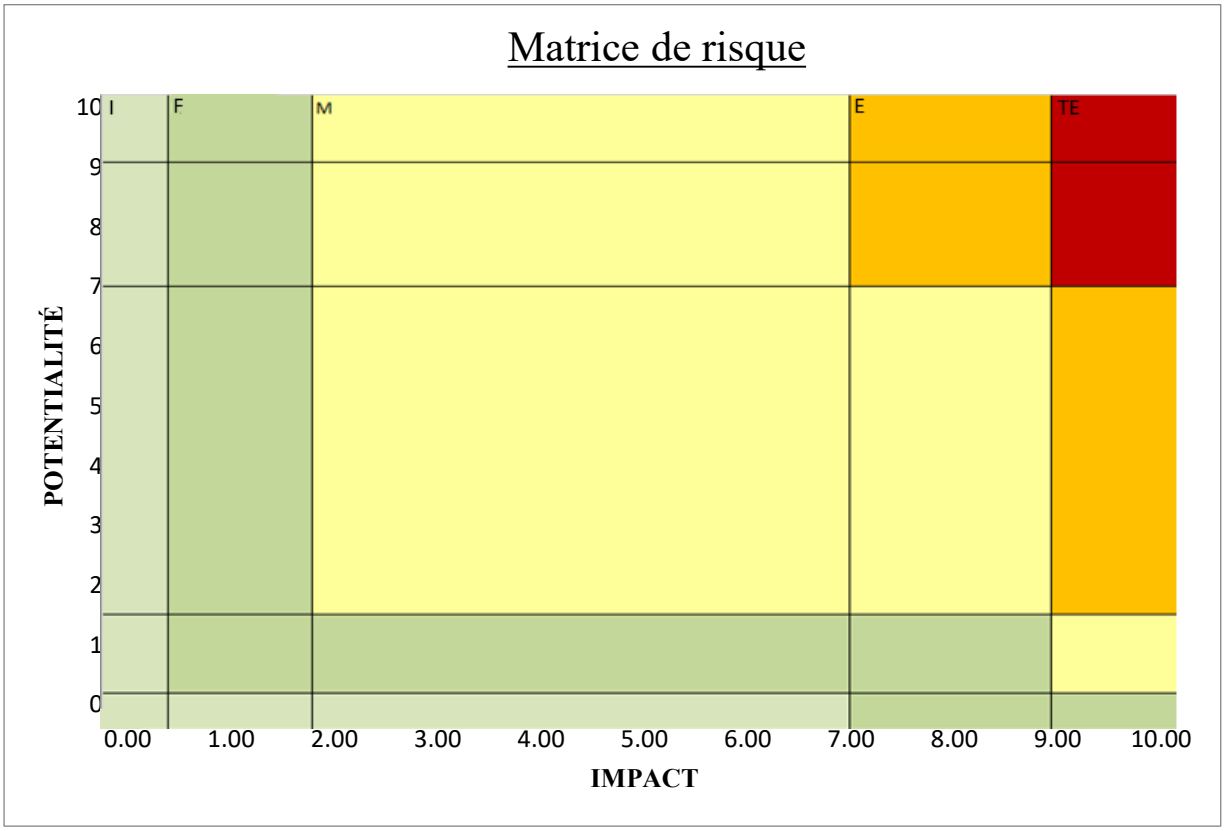

Figure 6-2 Modèle de référence - Matrice de risque

Les symboles présents sur la matrice (I, F, M, ...) sont simplement les premières lettres des niveaux de risque exposés dans la partie 6.4.3.

La plupart des vulnérabilités propres aux environnements de sécurité de l'information d'institutions bancaires/financières sont souvent évaluées avec un facteur d'actifs informationnels de type critique et de ce fait jouissent d'une catégorisation plus élevée en termes d'impact.

Ci-dessous le tableau permettant de résumer les scores de potentialité et d'impact pour chacune des vulnérabilités identifiées dans l'environnement de FINTRADE.

Tableau 6-5 Table de référence des vulnérabilités

ID	Name	Ensemble de vulnérabilité	Potentialité	Impact
T1	**Escalade de privilège à partir d'un poste de travail d'un employé typique**			
T1.1	Divulgation d'information de type GPP pour les mots de passe administratifs	EV 1	Modérée	Élevé
T1.2	Protocoles activés (LLMNR & NBTNS)	EV 1	Modérée	Modéré
T1.3	Signature SMB non obligatoire	EV 1	Modérée	Modéré
T1.4	Mots de passe faibles	EV 2	Modérée	Modéré

Tableau 6-5 Table de référence des vulnérabilités

T1.5	Les paramètres de proxy par défaut n'utilisant pas WPAD	EV 1	Modérée	Imperceptible
T2	**Chiffrement du poste de travail**			
T2.1	Attaque DMA	EV 3	Modérée	Élevé
T3	**Test Wi-Fi**			
T3.1	Absence d'isolation entre les utilisateurs sur le réseau Wi-Fi invité.	EV 1	Modérée	Modéré
T3.2	Détournement de session utilisateur sur FINTRADE visiteur	EV 7	Modérée	Modéré
T3.3	L'absence de filtrage entre les VLAN.	EV 7	Modérée	Modéré
T4	**Test d'ingénierie sociale**			
T4.1	Dispersion de clés USB	EV 4	Modérée	Modéré

Tableau 6-5 Table de référence des vulnérabilités

T5	**Test de sécurité physique**			
T5.1	Talonnage en zone restreinte	EV 4	Modérée	Modéré
T6	**Sécurité du processus de virtualisation**			
T6.1	Certaines données sont transférées entre la pré-production et la production	EV 6	Modérée	Modéré
T6.2	Compte d'ancien utilisateur non démissionné	EV 5	Modérée	Modéré
T7	**Sécurité du processus de sauvegarde**			
T7.1	Les données sont accessibles sur le site du fournisseur de solution	EV 3	Modérée	Modéré

Tableau 6-5 Table de référence des vulnérabilités

T7.2	Les sauvegardes ne peuvent pas être rétablies à temps (RTO)	EV 8	Modérée	Modéré
T8	**Tests de sécurité réseau**			
T8.1	Version non prise en charge de Windows Server 2003	EV 6	Modérée	Élevé
T8.2	Multiples vulnérabilités dans HP System Management Homepage	EV 6	Modérée	Élevé
T8.3	Vulnérabilités relatives aux configurations SSL/TLS	EV 3	Modérée	Modéré
T8.4	La signature SMB est désactivée	EV 1	Modérée	Modéré
T8.5	MITM sur Microsoft Windows Remote Desktop Protocol/Terminal Services	EV 1	Modérée	Modéré

Tableau 6-5 Table de référence des vulnérabilités

T8.6	L'authentification SMB de type session NULL	EV 1	Modérée	Modéré
T8.7	SSLv3 (POODLE)	EV 3	Modérée	Modéré
T8.8	Multiples vulnérabilités relatives à la configuration SSH	EV 3	Modérée	Faible

6.4.3 Évaluation des risques

L'évaluation des risques a permis de combiner des mesures d'impact et de potentialité pour produire un score de risque adapté avec le contexte de FINTRADE. De façon à baser notre système de référence qualitatif sur l'ensemble de cet exercice, il fut important d'afficher les matrices utilisées lors de l'évaluation et de la classification. Elles indiquent les différents niveaux de risques qualitatifs avec lesquels nous avons comparé la valeur numérique obtenue pendant le processus d'évaluation quantitatif. De façon à simplifier le processus d'évaluation, nous avons volontairement sauté l'étape de quantification de chaque vulnérabilité répertoriée.

6.4.3.1 Tableaux de référence pour l'évaluation du risque

6.4.3.1.1 Niveau des risques avec Contrôles Actuels (A/CA)

Ci-dessous le tableau de classification permettant d'appareiller les risques et de les évaluer selon un référentiel standardisé.

Tableau 6-6Échelle d'évaluation du risque (A/CA) – NIST SP800-30

Potentialité	Impact				
	Imperceptible	**Faible**	**Modéré**	**Élevé**	**Très élevé**
Très élevée	Imperceptible	Faible	Modéré	Élevé	Très élevé
Élevée	Imperceptible	Faible	Modéré	Élevé	Très élevé
Modérée	Imperceptible	Faible	Modéré	Modéré	Élevé
Faible	Imperceptible	Faible	Faible	Faible	Modéré
Imperceptible	Imperceptible	Imperceptible	Imperceptible	Faible	Faible

6.4.3.1.2 Niveau des risques résiduels avec Contrôles Recommandés (A/CR)

Tableau 6-7 Échelle de risque résiduel (A/CR) – NIST SP800-30

Risque A/CR	Efficacité du contrôle				
	Impercept.	**Faible**	**Modérée**	**Élevée**	**Très élevée**
Très élevé	Très élevé	Très élevé	Très élevé	Élevé	Faible
Élevé	Élevé	Élevé	Élevé	Modéré	Faible
Modéré	Modéré	Modéré	Modéré	Faible	Impercept.
Faible	Faible	Faible	Faible	Impercept.	Impercept.
Impercept.	Impercept.	Impercept.	Impercept.	Impercept.	Impercept.

Dans ce tableau, Imperceptible est réduit à « Impercept. »

Les tableaux exposés pour la classification sont tirés du NIST et plus particulièrement du standard SP800-30.

6.4.3.2 Classification des vulnérabilités selon les échelles de risque

Voici un extrait de la classification des vulnérabilités selon les échelles et matrice de risque :

Tableau 6-8 Classification des vulnérabilités

ID	Name	Ensemble de vulnérabilités	Potentialité	Impact	Risque A/CA	Risque A/CR
T1	**Escalade de privilège à partir d'un poste de travail d'un employé typique**					
T1.1	Divulgation d'information de type GPP pour les mots de passe administratifs	EV 1	Modérée	Élevé	Modéré	Faible
T1.2	Protocoles activés (LLMNR & NBTNS)	EV 1	Modérée	Modéré	Modéré	Faible

Pour la totalité du tableau de classification, veuillez vous référer à l'annexe D.

6.4.3.3 Niveaux de risques avec contrôles actuels (A/CA)

Le tableau suivant répertorie les niveaux de risques en fonction des ensembles de vulnérabilités ayant été attribués suite aux activités de tests d'intrusion (Avec Contrôles Actuels). Par conséquent, ce tableau reflète les risques en se basant sur les contrôles de sécurité actuels.

Tableau 6-9 Niveaux des risques inhérents

ID	Catégorie de contrôle	Risque avec contrôle actuel (A/CA)
EV 1	Configuration	Modéré
EV 2	Gestion de l'authentification	Modéré
EV 3	Mesures cryptographiques	Modéré
EV 4	Intrusion physique	Modéré
EV 5	Contrôles d'accès, permission et privilèges	Modéré
EV 6	Erreurs de gestion	Élevé
EV 7	Fonctionnalité de sécurité	Modéré
EV 8	Manipulation des supports de données	Modéré

Ce tableau reflète la matrice d'ensemble de vulnérabilités évaluées avec contrôles actuels, qui est présentée ci-dessous :

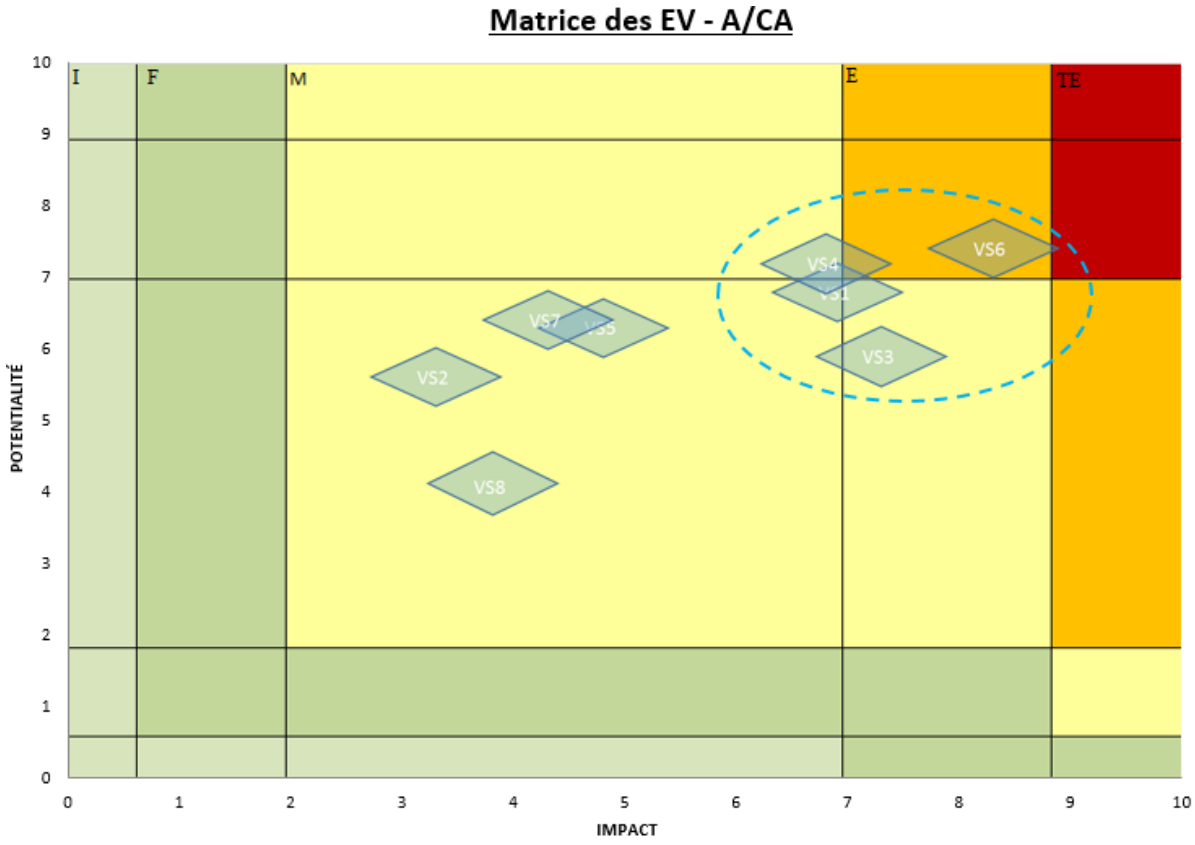

Figure 6-3 Matrice EV - A/CA.

Les EV sont identifiés dans la figure par l'acronyme anglais VS (« Vulnerability Set »).

Le niveau approprié pour chaque ensemble de vulnérabilités fut une combinaison de la plus haute valeur relative à l'impact potentiel de l'ensemble de la vulnérabilité inclus respectivement dans ces jeux de vulnérabilités.

Pour rappel, l'attribution qualitative d'une classe de risque (EV) a été établie en fonction du :

- Facteur de potentialité pour un ensemble de vulnérabilités donné étant égal à la valeur du facteur de potentialité le plus élevé des vulnérabilités composant l'ensemble.
- Facteur d'impact pour un ensemble de vulnérabilités donné étant égal à la valeur moyenne des facteurs d'impact de chaque vulnérabilité composant l'ensemble.

6.4.3.4 Niveaux de risque résiduel avec contrôles recommandés (A/CR)

Le tableau suivant présente les risques résiduels quantifiés (Avec Contrôles Recommandés) suite à l'application des contre-mesures découlant des contrôles recommandés (A/CR).

Les niveaux de risques résiduels furent évalués selon l'hypothèse que chaque ensemble de vulnérabilités comportait un risque résiduel de par l'implantation du contrôle et des contre-mesures découlant des recommandations du rapport de tests d'intrusion.

Suite aux calculs de réduction des vulnérabilités, les ensembles de vulnérabilités furent réévalués (selon la table RR-1) quantitativement et qualitativement de façon à obtenir les niveaux de risques associés.

Tableau 6-10 Niveaux des risques résiduels

ID	Catégorie de contrôle	Risque avec contrôle recommandé (A/CR)
EV 1	Configuration	Faible
EV 2	Gestion de l'authentification	Faible
EV 3	Mesures cryptographiques	Modéré
EV 4	Intrusion physique	Modéré
EV 5	Contrôles d'accès, permission et privilèges	Faible
EV 6	Erreurs de gestion	Faible
EV 7	Fonctionnalité de sécurité	Faible
EV 8	Manipulation des supports de données	Faible

Ce tableau reflète la matrice d'ensemble de vulnérabilités évaluées avec contrôles recommandés, qui est présentée ci-dessous :

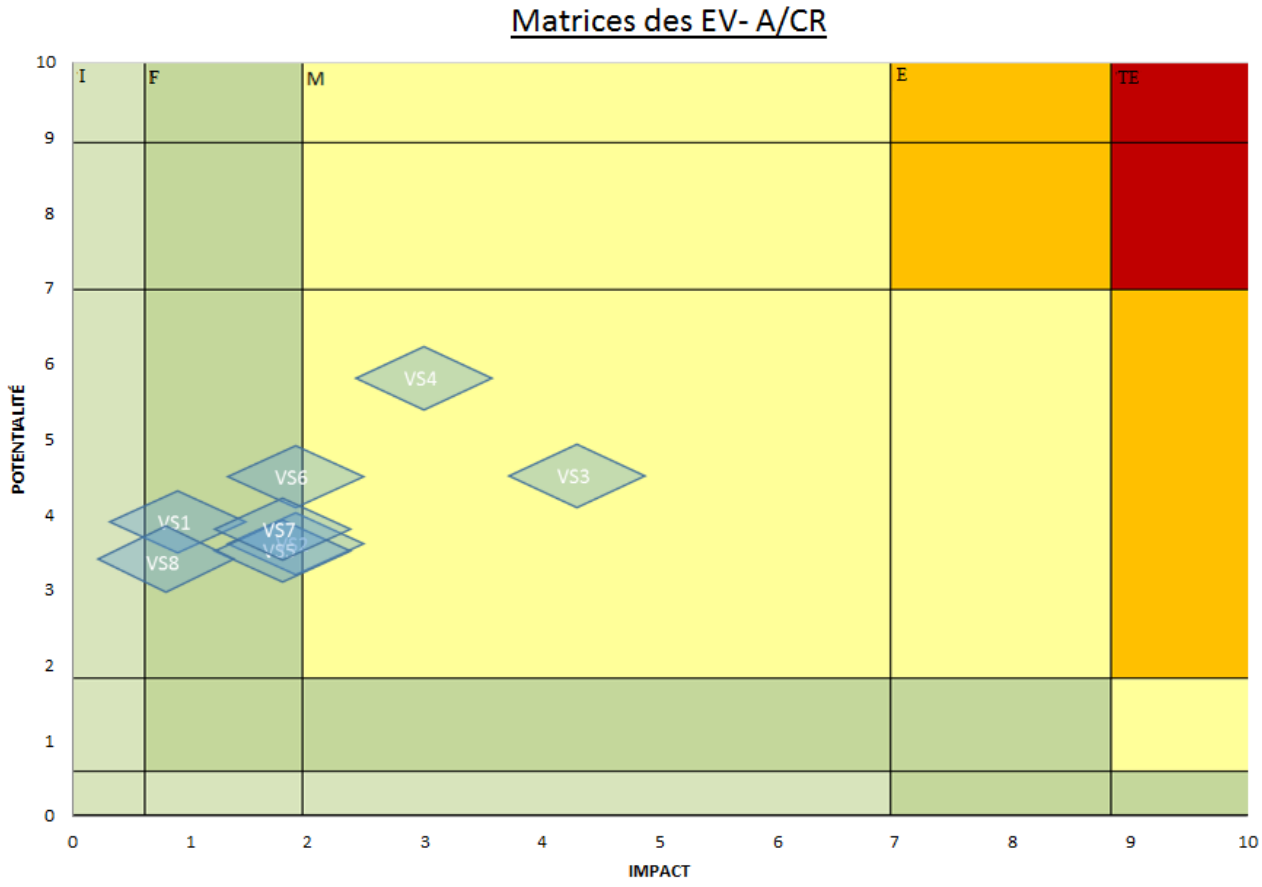

Figure 6-4 Matrice EV - A/CR.

Les EV sont identifiés dans la figure par l'acronyme anglais VS (« Vulnerability Set »).

6.4.3.5 Table de comparaison des risques résiduels

Ci-dessous, le tableau permet de recenser les ensembles de vulnérabilités selon les deux niveaux de risque présentés précédemment, en ajoutant la notion de priorisation et de référence relative aux contrôles. Les niveaux de priorité ont été établis selon deux facteurs :

- Le différentiel obtenu entre les niveaux A/CA et A/CR obtenus lors de l'étape de traitement.
- Le nombre de vulnérabilités contenues dans l'EV ainsi que leur sévérité.

Les contrôles identifiés et tirés du référentiel choisi (NIST SP800), ont permis d'indiquer quels sont les contrôles et contre-mesures à implémenter pour atteindre les cibles de risque résiduel.

Tableau 6-11Traitement par Ensemble de Vulnérabilité (EV)

ID	Catégorie de contrôle	Niveau de risque avec contrôle actuel (W/AC)	Niveau de risque résiduel (W/CR)	Phase de priorité de traitement	Controls NIST (SP800)
EV 1	Configuration	Modéré	Faible	P1	CM-2(1),CM-2(7),SC-22,AC-18(1), AC-17(2)
EV 2	Gestion de l'authentification	Modéré	Faible	P2	IA-5(4), CM-6
EV 3	Mesures cryptographiques	Modéré	Modéré	P3	CM-3(6),SC-13(1)
EV 4	Intrusion physique	Modéré	Modéré	P3	AT-2(2), AC-20(2)
EV 5	Contrôles d'accès, permission et privilèges	Modéré	Faible	P1	AC-2, AU-6
EV 6	Erreurs de gestion	Élevé	Faible	P1	CM-2(1), CM-2(2)
EV 7	Fonctionnalité de sécurité	Modéré	Faible	P2	AC-18(1), SC-7
EV 8	Manipulation des supports de données	Modéré	Faible	P2	CP-9(2)

6.4.4 **Priorité de traitement**

Ci-dessous, nous exposons le tableau de priorisation. Suite à cela, le détail des explications est fourni.

Tableau 6-12 Priorité de traitement

ID	Catégories de contrôle	Phase de priorité de traitement
EV 1	Configuration	P1
EV 2	Gestion de l'authentification	P2
EV 3	Mesures cryptographiques	P3
EV 4	Intrusion physique	P3
EV 5	Contrôles d'accès, permission et privilèges	P2
EV 6	Erreurs de gestion	P1
EV 7	Fonctionnalité de sécurité	P2
EV 8	Manipulation des supports de données	P2

P1 Mitigation de premier plan:

Les ensembles de vulnérabilités correspondant au tiers P1 ont dû obligatoirement être traités le plus rapidement possible avec les contrôles et contre-mesures appropriés. Les contrôles, comme identifiés dans le tableau, ont permis d'induire une réduction de risque majeure et furent donc qualifiés de hautement effectifs. En référence à la matrice de classification, EV 6 est caractérisé par une réduction de risque passant d'Élevé à Faible. Cela implique donc une réduction de deux niveaux sur l'échelle d'évaluation qualitative préconisée par le NIST.

Selon les caractéristiques principales d'EV1 concernant les configurations, et de par la représentation majoritaire des vulnérabilités dans ce groupement en particulier (35%), nous avons

pu le classifier comme étant un des ensembles de haute priorité de traitement. EV 1 est aussi caractérisé par une réduction de risque passant de Modéré à Faible. De ce fait, le processus de traitement immédiat des risques sur ces ensembles a permis d'atteindre une réduction représentant 48% du total de vulnérabilités identifiées.

P2 Mitigation de deuxième plan:

Suite au traitement des ensembles 1 et 6, la deuxième phase de traitement commença en se concentrant sur les EV 2, 5, 7 et 8. La raison repose dans la facilité de traitement de ces ensembles.

Comme il est possible de le constater, la majorité des risques furent représentés à travers la catégorie 0604 concernant la divulgation d'information. Les contrôles concernant cette catégorie sont considérés comme effectifs grâce à leur action de réduction. Cette deuxième phase de traitement se concentra sur l'implantation d'un programme de gestion des mises à jour et de gestion des versions et configurations, de façon à mitiger les vulnérabilités contenues dans les ensembles cités plus haut. Les efforts relatifs à la mise en place du programme furent considérés comme faibles. La mitigation effectuée lors de cette phase aura permis une réduction des risques de 67 % sur le total identifié.

P3 Mitigation de troisième plan:

Les EV 3 et 4 rassemblaient des risques dont le traitement nécessiterait des investissements lourds ainsi qu'une formation avancée en sécurité de l'information pour les employés de l'entreprise FINTRADE. Quand bien même les matrices de risque indiquent une décroissance d'impact et de sévérité pour ces ensembles, suite aux mesures de traitement, les risques résiduels n'ont pas permis d'obtenir une réduction suffisante pour être qualifiée de Faible. C'est donc pour cela que la priorisation de ces ensembles est effectuée en dernier.

6.4.5 **Répartition des risques**

Ci-dessous les indicateurs relatifs aux EV.

6.4.5.1 Par ensemble de vulnérabilité

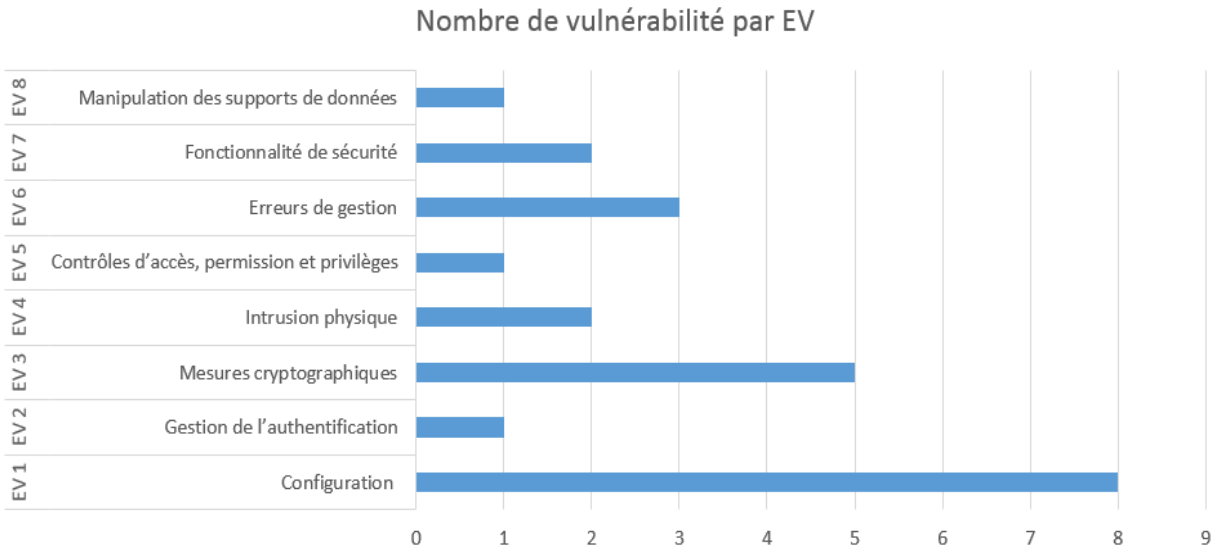

Figure 6-5 Diagramme en bâton - Distribution des EV

6.4.5.2 Par activité de tests d'intrusion

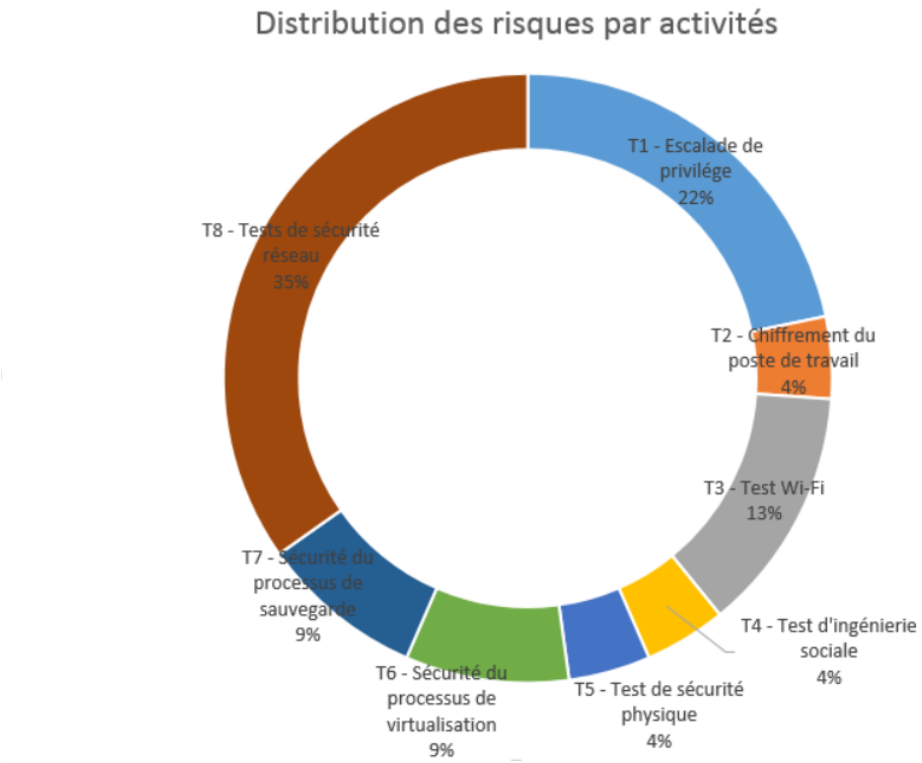

Figure 6-6 Diagramme circulaire exposant la répartition des vulnérabilités par activités

6.5 Processus d'amélioration continue (PAMC)

6.5.1 Indicateurs de sécurité

Ci-dessous sont exposés les indicateurs relatifs à l'exercice d'évaluation de risque. Ils ont permis d'établir une base d'indicateurs axés sur la posture de sécurité de l'entreprise et de son environnement numérique. L'amélioration continue fut donc initiée en prenant en compte les valeurs suivantes pour établir un suivi régulier et efficace lors des prochains tests d'intrusion :

- Répartition totale
- Distribution de potentialité
- Distribution d'impact
- Distribution de risque
- Catégorie de perte de données.

6.5.1.1 Répartition totale

La figure de répartition totale des risques permet d'apprécier la posture générale relative aux risques quantifiés. La majorité de notre échantillonnage de risque A/CA est classée en catégorie modérée avec une proportion de 86 %. Suite au traitement et implantation des contre-mesures, l'évaluation des risques résiduels permet d'obtenir une proportion de 82 % des risques appartenant à la catégorie faible.

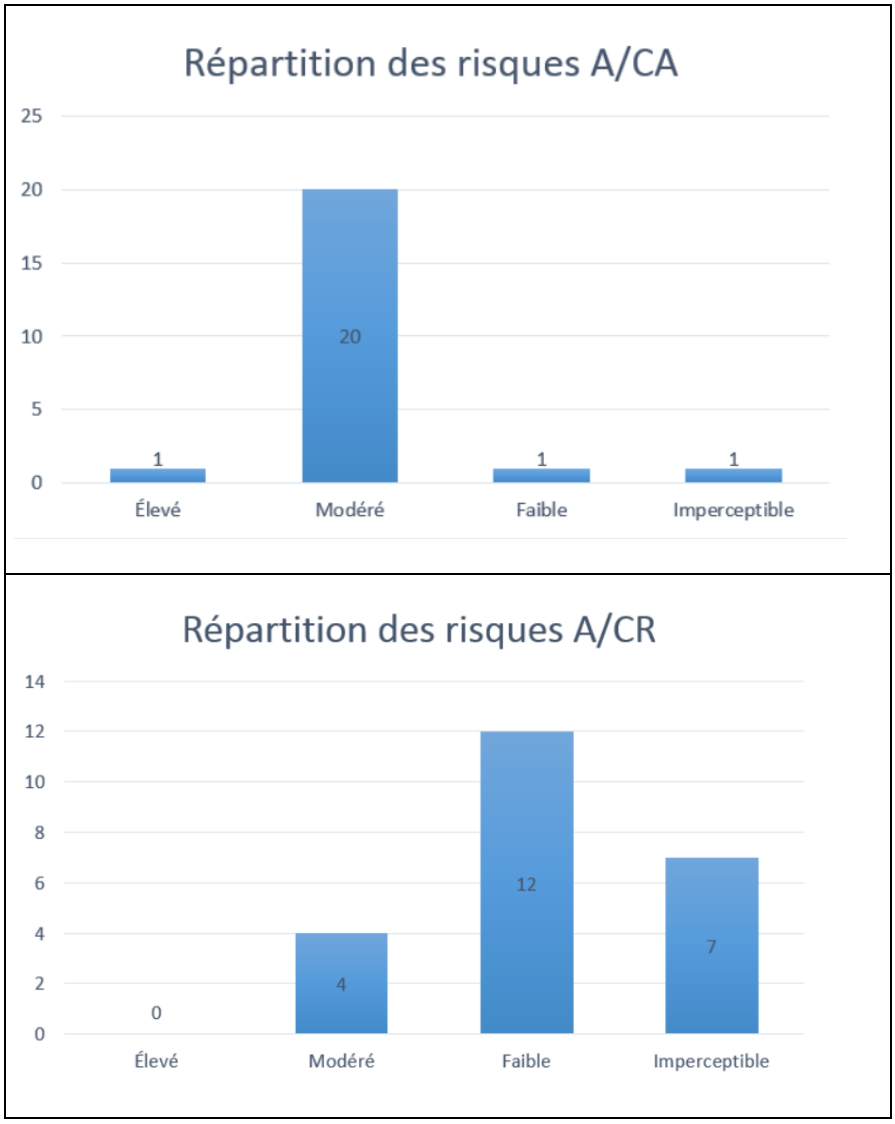

Figure 6-7 Répartition des risques A/CA & A/CR

6.5.1.2 Distribution de potentialité

Ci-dessous les valeurs de potentialité pour chacun des risques identifiés. La comparaison des diagrammes A/CA et A/CR permet de montrer une diminution quant aux valeurs de potentialité.

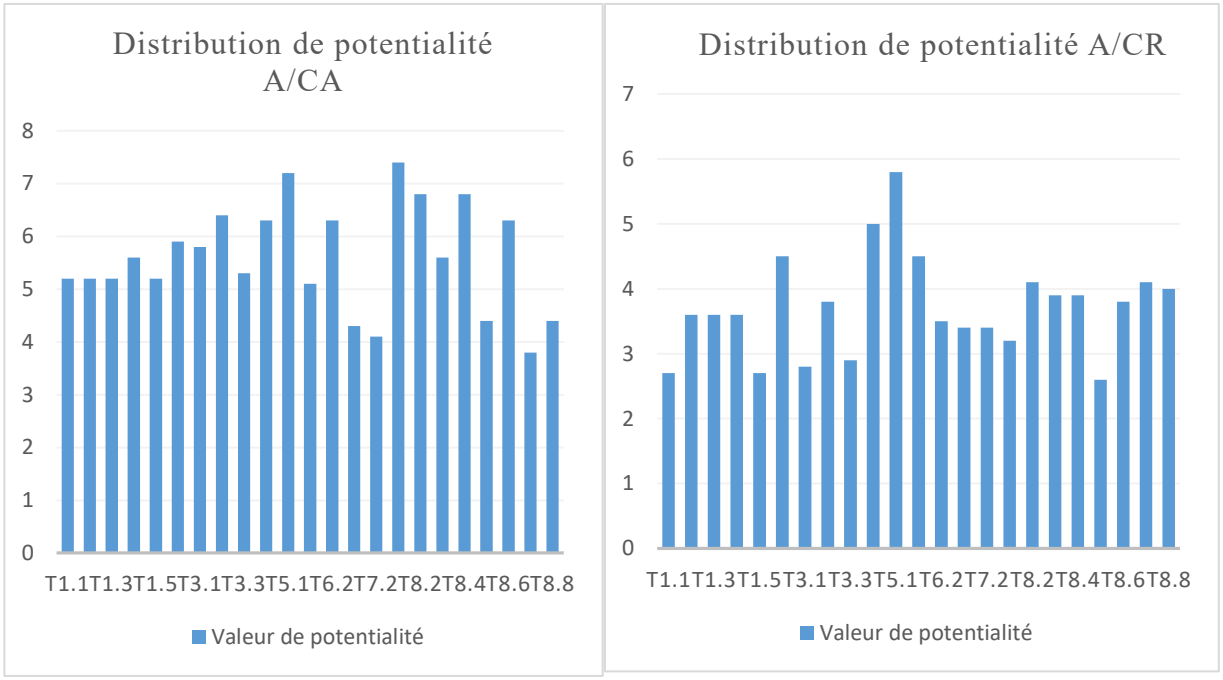

Figure 6-8 Comparaison entre les distributions avant et après traitement

6.5.1.3 Distribution d'impact

Ci-dessous, les valeurs d'impact pour chacun des risques identifiés. En prenant en compte que la majorité des risques évalués sont liés à des vulnérabilités logiques et facilement remédiables, la réduction d'impact est beaucoup plus prononcée.

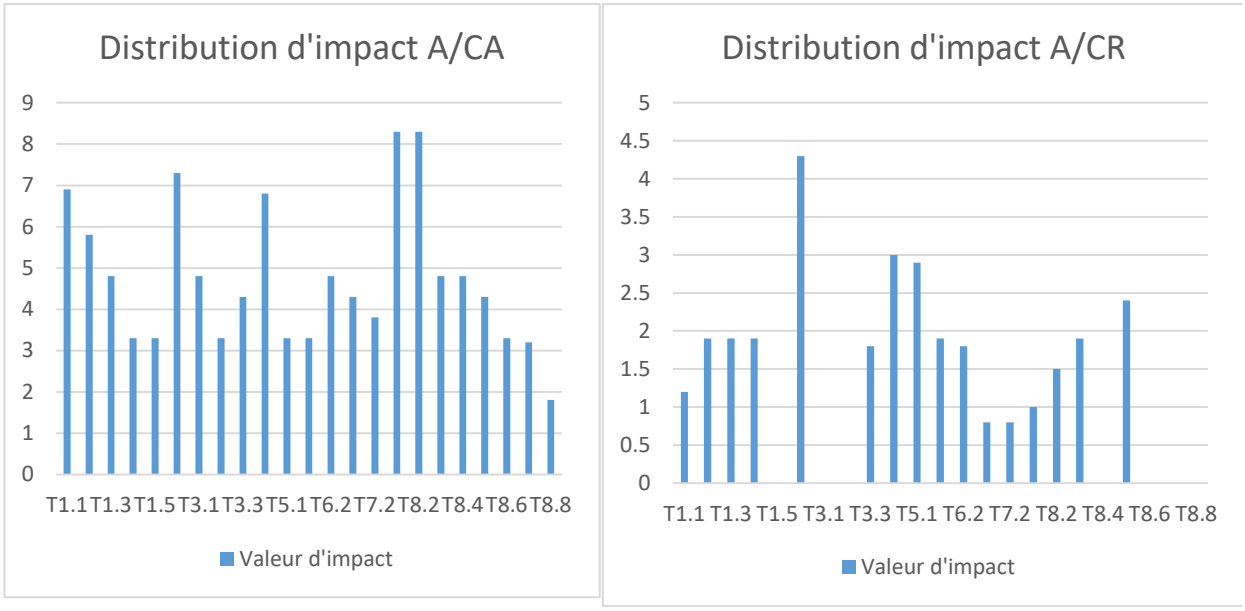

Figure 6-9 Comparaison entre les distributions d'impact avant et après traitement

6.5.1.4 Distribution de risque

Ci-dessous, le diagramme de distribution des risques avec contrôles actuels.

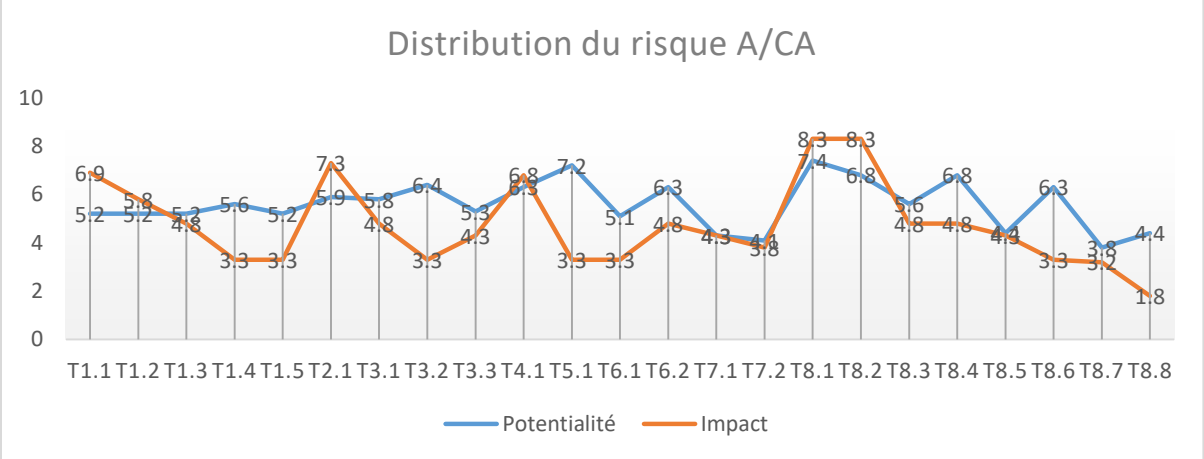

Figure 6-10 Distribution du risque A/CA

Ci-dessous, le diagramme de distribution des risques avec contrôles recommandés. On observe bien les effets de réduction des contrôles.

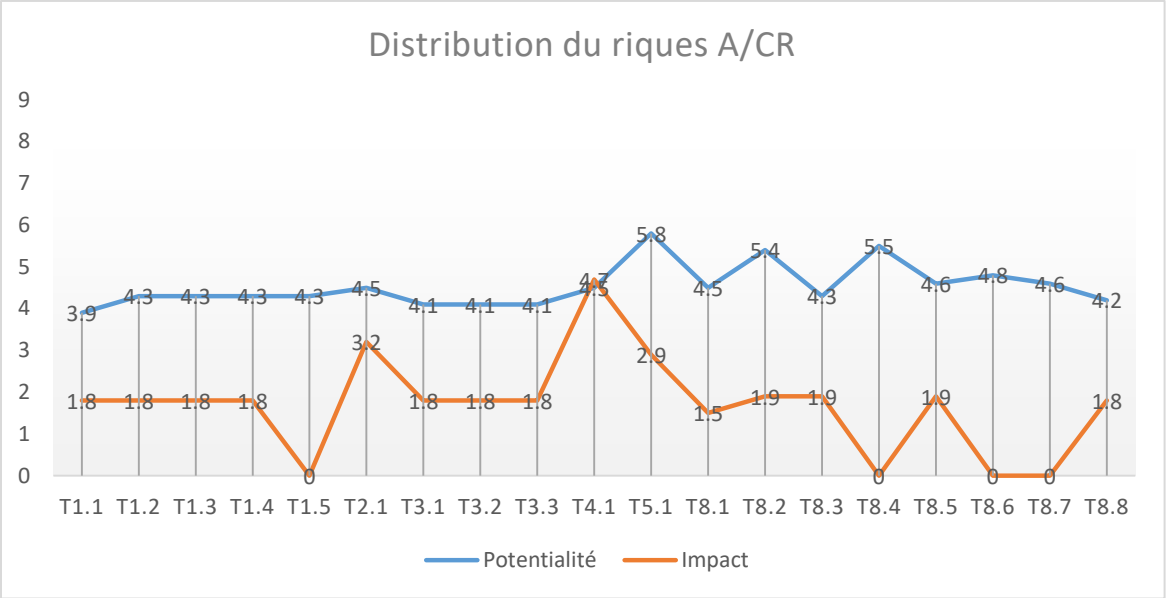

Figure 6-11 Distribution du risque A/CR

6.5.1.5 Catégorie de divulgation de données

Le diagramme ci-dessous permet de refléter la répartition des scénarios énumérés et suggérés par le département de sécurité de l'information de FINTRADE.

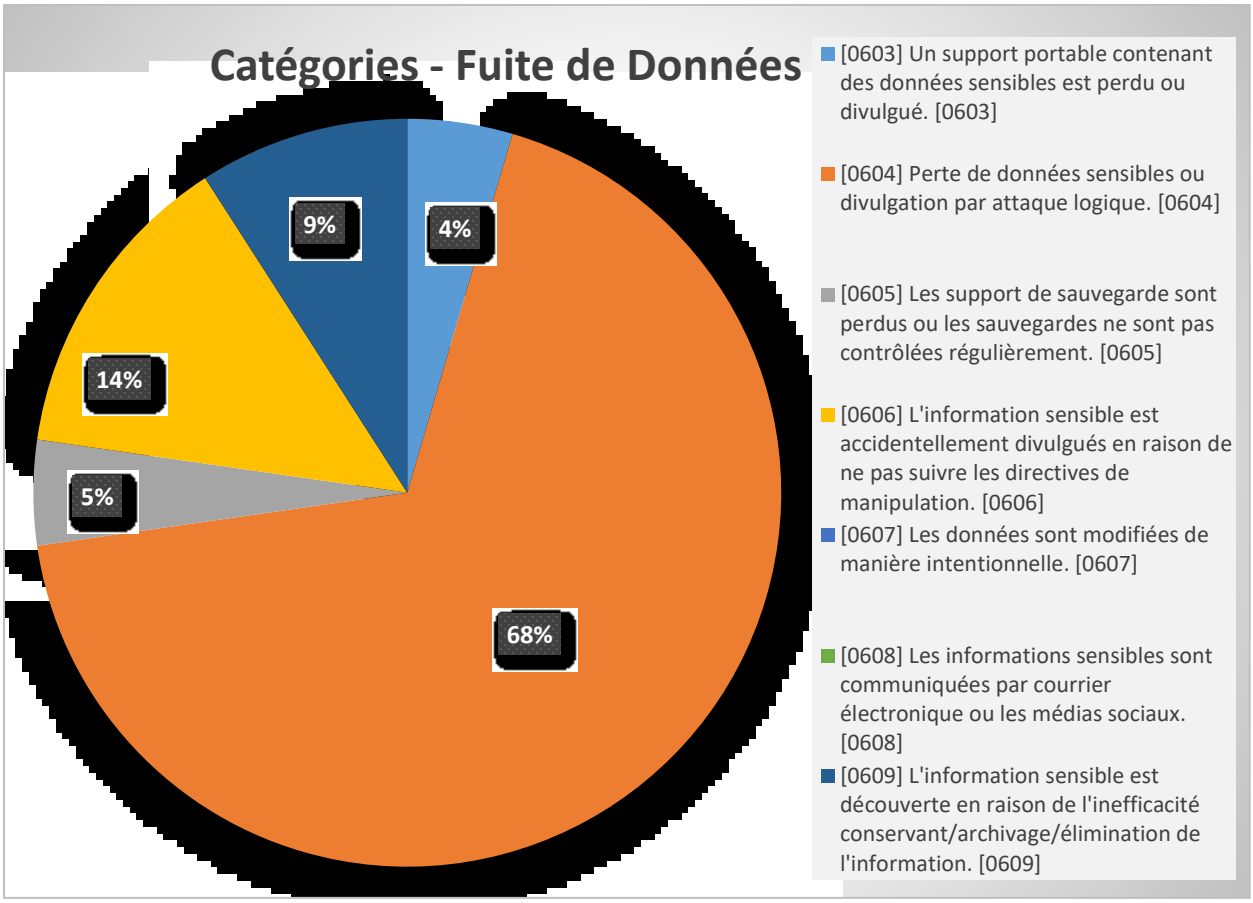

Figure 6-12 Catégories - Fuite de données

Cette observation permet de constater que la majorité des risques appartient à la catégorie de divulgation par attaque logique.

6.5.2 **Recommandations générales– Zone à Haut Risque**

Dans cette section, nous présenterons les recommandations sous la forme d'une description globale du contrôle de sécurité qui fut mis en œuvre de manière à répondre aux risques les plus élevés, et identifiés dans l'environnement de FINTRADE. Nous avons identifié quatre (4) EV qui représentent la zone à risque la plus élevée.

6.5.2.1 EV 1 – Gestion de la configuration

Priorité : P1

Description:

Trente-cinq pourcents (35%) des vulnérabilités identifiées sont liées à des problèmes de configuration. Il a été fortement recommandé d'examiner la gestion de la configuration de sécurité ainsi que les pratiques de durcissement des systèmes et les paramètres de configuration de la sécurité. Une partie de la vulnérabilité découverte par les tests d'intrusion résulte d'une configuration de sécurité erronée qui exposait les systèmes d'information de FINTRADE aux attaquants. La première priorité a été déterminée en raison des deux niveaux d'écart de réduction des risques, constatée grâce à la contre-mesure et aux contrôles applicables à cet EV. En outre, l'atténuation de ces risques fut très efficace et facile à mettre en œuvre.

6.5.2.2 EV 3 – Problèmes de cryptographie

Priorité P3

Description:

Certaines des versions des technologies et protocoles utilisés dans le réseau interne avaient des vulnérabilités qui auraient pu permettre à un attaquant expérimenté de briser la sécurité du canal en exploitant des algorithmes cryptographiques désuets. Bien qu'il fût recommandé de mettre à jour et corriger les systèmes concernés, il était également essentiel de les adapter et de tenir compte des exigences de compatibilité dans l'environnement FINTRADE. Cela justifia le choix de placer cet ensemble sur la troisième priorité aussi parce que le risque résiduel, avec les contrôles recommandés, se situe toujours à un niveau modéré. Les risques associés doivent être régulièrement examinés et contrôlés.

6.5.2.3 EV 4 – Intrusions physiques

Priorité P3

Description:

Afin de protéger les informations internes et de limiter les actions défavorables d'intrus, il fut recommandé de maintenir une session de formation régulière pour sensibiliser les employés à la sécurité des informations et aux meilleures pratiques. En outre, il est important que les employés

signalent tout comportement inhabituel et se renseignent sur l'identité du personnel inconnu ou non identifié. Cette EV fut catégorisée en troisième priorité parce qu'elle nécessiterait des contrôles d'atténuation physique très coûteux de manière à être réduite à un niveau bas.

6.5.2.4 EV 6 – Erreurs de gestion des ressources

Priorité P1

Description:

La vulnérabilité concernée dans cette EV aurait pu avoir un impact important si des informations étaient sur le point d'être divulguées ou interceptées. Cet ensemble de vulnérabilités concerne des processus tels que la gestion des correctifs, les mises à jour et les mises à niveau des systèmes. Pour faire face aux risques liés à cette partie, il fut essentiel d'améliorer la politique de contrôle des changements en révisant et en actualisant régulièrement les systèmes d'information désuets. En outre, ces systèmes ont dû être séparés de l'accès au réseau interne et régulièrement testés. L'utilisateur interne ordinaire ne doit pas pouvoir accéder à ces serveurs. En conséquence, nous avons décidé de donner la priorité de premier niveau à cette EV. Il fut fortement recommandé de traiter et d'atténuer rapidement les risques associés.

Suite à la présentation des résultats de priorisation, les EV en question furent traités selon la priorité énoncée dans le contexte. Le plan de priorisation fut présenté et approuvé dès la fin de la présentation par la responsable du département de sécurité de l'information. Cette mesure visait à implémenter le plus rapidement possible les traitements, de façon à présenter une réduction aux auditeurs, présents pour un exercice d'audit externe.

6.6 Limitations de l'étude de cas et discussion

Le contexte du client indique un environnement mature lié à l'organisation et à la gestion des processus et des risques d'entreprise. L'objectif principal de cette évaluation du risque était de déterminer les priorités de traitement et les contrôles d'atténuation après le processus de tests d'intrusion. De cette façon, la méthodologie ITREM a été introduite pour regrouper toutes les données techniques disponibles et relatives aux rapports des tests d'intrusion. Ainsi, toute la

classification des données et la capacité de priorisation de la méthodologie ont été personnalisées pour produire les résultats escomptés.

L'évaluation des risques effectuée dans le cadre de cet exercice visait à fournir des données tangibles concernant la découverte et l'analyse des vulnérabilités relatives à la sécurité de l'information. Bien que nous ayons énuméré plusieurs activités d'examen de la sécurité (T6, T7), nous n'avons pas évalué d'autres éléments de l'environnement numérique susceptibles d'avoir une incidence sur la confidentialité, la disponibilité et l'intégrité des systèmes. Nous n'avons tenu compte que des risques associés aux vulnérabilités identifiées dans les activités liées à la portée du rapport de tests d'intrusion.

Lors du projet, FINTRADE et son département de sécurité ont été engagés dans de nombreuses discussions avec OKIOK pour définir la portée des tests ainsi que celle de l'exercice d'évaluation des risques.

La raison était principalement dû au fait que le département avait déjà une méthodologie d'évaluation des risques. Cependant, cette dernière n'était en aucun cas calquée sur une approche similaire à ITREM. De plus, la responsable du département avait des enjeux relatifs aux résultats de l'évaluation, car ces derniers allaient confirmer certaines parties très à risque de l'environnement numérique de FINTRADE. Il y'avait donc un enjeu de politique d'entreprise pour ne pas montrer immédiatement les risques et privilégier un traitement prioritaire avant de présenter les résultats au comité exécutif de l'entreprise. Un des points sortant de cette discussion fut la validation du plan de traitement et l'application de ce dernier de façon immédiate pour pouvoir palier aux risques le plus rapidement possible.

De plus, le département de sécurité de FINTRADE était aussi curieux de savoir la complexité du processus méthodologique ainsi que de la charge potentielle répercutée sur les équipes opérationnelles pour effectuer le traitement des risques identifiés. La partie d'appréciation du contexte fut cruciale pour déterminer les catégories de classification des risques et leur appareillage sous-jacent.

Suite à l'exercice d'évaluation, nous avons donc demandé à l'équipe de FINTRADE de nous donner leur ressenti sur le déroulement du processus méthodologique et l'acuité des résultats.

À cet effet nous avons axé leur réponse sur trois points principaux :

- La complexité du processus méthodologique
- L'efficacité de ce dernier
- L'applicabilité

La complexité du processus a pu être qualifiée de simple, tant et pour autant qu'un guide méthodologique expliquait les étapes précises permettant de passer de l'identification des risques au traitement de ces derniers. L'équipe de FINTRADE n'a pas eu de problème à reprendre certaines parties de la méthodologie pour les appliquer et ajuster certains indices.

L'efficacité a été mesurée tant par les coûts monétaires engendrés par les projets de rehaussement des contrôles de sécurité, permettant le traitement des risques, que par les estimés effectués par la responsable de la sécurité de FINTRADE. Comme mentionné par cette dernière, pour le même budget annuel alloué aux traitements des risques, nous avons pu traiter 4 initiatives de sécurité additionnelles en comparaison à une année où les tests d'intrusions n'avaient pas été évalués et priorisés. Cette augmentation dans la réalisation du nombre d'initiatives permet d'appuyer la dimension d'efficacité propre à la méthodologie.

L'applicabilité fut très fluide, car nous avions effectué une adaptation au contexte d'affaires et au cadre normatif. La responsable du département de sécurité ainsi que les membres de son équipe auraient été très surpris et dépités si cette étape n'avait pas été prise en compte pour effectuer l'évaluation.

Globalement, FINTRADE et son équipe ont été très satisfaits par la mise en place d'ITREM et des résultats en découlant. L'entreprise a apprécié la valeur ajoutée découlant des dimensions d'adaptabilité, de flexibilité, et de priorisation induite par l'application d'une méthodologie d'évaluation des risques basée sur les tests d'intrusion. Cette étude de cas fut donc probante pour le cas de FINRADE en particulier. Cependant, pour assurer une certaine stabilité du modèle opérationnel de la méthodologie, il serait nécessaire de rassembler une cinquantaine d'études de cas. Cela permettrait d'extraire les données de vulnérabilités selon certains segments d'affaires et assurerait par ce biais une contre-validation du modèle de gestion des risques pour de futures applications de la méthodologie. De plus, une base conséquente d'études de cas permettrait de

raffiner le degré d'attribution des facteurs de calcul de risque. La pondération des facteurs pourrait aussi entrainer un biais d'analyse au cas où les poids venaient à être attribués sans guidage particulier. Les travaux et développent futurs, notamment grâce à une base grandissante des études de cas, s'orienteront vers un croisement des risques principaux identifiés et les contrôles de sécurité à appliquer pour arriver à un traitement optimal du risque.

CHAPITRE 7 CONCLUSION ET RECOMMANDATIONS

ITREM est une méthodologie permettant d'unifier le traitement des risques relatifs aux vulnérabilités des systèmes d'information. Elle doit être perçue comme un effort de liaison entre plusieurs processus d'entreprise, venant conforter l'aspect propre à la sécurité de l'information, notamment les processus de découvertes de vulnérabilités à travers les tests d'intrusion, l'évaluation de risques informatiques, et la sélection de contrôles de sécurité permettant de réduire ces risques. De ce fait, elle permet d'achever l'unification des efforts de gestion et de conformité technique et légale. Elle permet aussi d'apporter un aspect de priorisation aux scénarios de risque traditionnels que l'on retrouvera en entreprise.

En contraste avec les méthodologies d'évaluation de risques traditionnelles qui se basent sur des évaluations subjectives de potentialité et des impacts de scénarios génériques, déterminés par des analystes de sécurité, ITREM se base sur les résultats objectifs des tests d'intrusion communément utilisés dans la pratique professionnelle pour répertorier de réelles vulnérabilités sur les systèmes informatiques. Une autre de ces caractéristiques est de pouvoir créer des indicateurs de gestion et de priorisation en appliquant des contrôles de sécurité, tirés de plusieurs référentiels internationaux, de façon à guider les équipes de sécurité de l'information à travers des recommandations entièrement adaptées au contexte de l'entreprise. En effet, la majorité des méthodologies actuelles n'offrent pas de priorisation des traitements suite à la catégorisation des risques évalués sur un environnement donné. En plus de la dimension subjective qu'apportent souvent les évaluations qualitatives par scénarios, les méthodologies de gestion des risques ne présentent que peu de moyens pour influencer les facteurs d'impact et de potentialité selon une pondération adaptée au contexte d'affaires.

À cet effet, nous avons adressé notre première question de recherche en indiquant comment prendre en compte le contexte d'une vulnérabilité, afin de la catégoriser en termes de niveau de risque. Cet aspect de la méthodologie ITREM est capturé dans le Processus d'appréciation du contexte (PAC).

Nous avons également adressé la deuxième question de recherche, concernant la standardisation des extrants des tests d'intrusion, en décrivant dans notre Processus de tests d'intrusion (PTI)

comment ces résultats doivent être standardisés et traités de façon à être utiles aux étapes subséquentes d'ITREM.

Afin d'augmenter la viabilité d'ITREM en termes d'efforts, nous avons développé le *Vulnerability Analysis Scoring System* (VANSS) qui nous permet de systématiser la classification des vulnérabilités. Nous avons construit un classificateur automatisé en employant des techniques d'apprentissage machine, notamment la régression logistique et les *Support Vector Machine* (SVM), qui nous ont permis d'atteindre des taux de précisions de près de 80%. Cela n'est pas probant d'un point de vue scientifique, mais est quand même encourageant dans un contexte d'affaires dans lequel la seule alternative actuelle est une classification subjective, arbitraire et coûteuse par un expert analyste de sécurité.

Finalement, nous avons cherché à évaluer l'efficacité et la viabilité d'ITREM de façon globale en adressant notre quatrième question de recherche à travers une étude de cas correspondant à l'utilisation d'ITREM dans un cas réel en entreprise, notamment dans l'institution que nous avons dénommée FINTRADE, afin de protéger son identité. Plus concrètement, nous avons mis de l'avant la possibilité d'obtenir un niveau de précision accru quant à l'identification, l'analyse, l'évaluation, et la prise de décision par rapport à l'évaluation du risque et la sélection des contrôles de sécurité à déployer pour protéger les systèmes informatiques. Il n'est pas possible, avec le niveau de maturité actuel de la méthodologie, de pouvoir conclure sur l'aspect décisionnel et son amélioration. Il faudrait pour cela bénéficier d'une étude comparative avec plusieurs dizaines d'entreprises participantes sur lesquelles ITREM aurait été déployée. Ces dernières seraient comparées en prenant en compte une gestion de la sécurité informatique avec et sans ITREM, suite à des tests d'intrusions. Cela permettrait d'obtenir des données précises sur l'avantage décisionnel lié à la méthodologie.

Néanmoins, l'étude de cas a permis de prouver qu'ITREM se différencie grâce à son caractère original et selon les propriétés suivantes :

- Adaptable à tout résultat et rapport de tests d'intrusion;
- Basée sur des facteurs de risque plus précis que ceux employés par CVSS;

- Flexible et rapide à utiliser;
- Fournit plusieurs indicateurs relatifs à la posture de sécurité de l'entreprise;
- Favorise le traitement des risques à travers une optique de réduction de la posture de risque et des recommandations précises et priorisées.

Une des valeurs ajoutées de la méthodologie se traduit par l'agrégation des vulnérabilités et des risques associés, en groupe ou catégorie (EV). Cette catégorisation reprenant les caractéristiques communes des vulnérabilités, elle permet d'associer des contrôles de traitement de façon à fournir des mesures palliatives agissant de concert pour éliminer tout risque associé à l'ensemble de vulnérabilité. Le processus de regroupement n'est que très peu implémenté actuellement en entreprise, et gagnerait à être plus utilisé de façon à raccourcir les temps de traitement alloués aux plans de correction concernant les vulnérabilités.

Les tests d'intrusion sont donc des exercices permettant d'obtenir des informations extrêmement précises et bénéfiques pour une entreprise soucieuse de la qualité de son approche en termes de prévention face aux menaces et attaques informatiques. Le processus de tests d'intrusion ne doit cependant pas être limité à de simples balayages automatisés permettant de déceler les vulnérabilités publiquement annoncées. Il doit être effectué de manière très personnalisée, en prenant majoritairement en compte les aspects technologiques de l'environnement client et l'exposition potentielle des actifs informationnels à travers les solutions et services inclus dans la portée des tests.

Une des limitations propres à la méthodologie est d'ailleurs relative à la portée. Il n'est pas possible, sauf pour une entreprise disposant de moyens et de temps suffisants, d'inclure la portée de l'entreprise englobant la totalité de son environnement numérique et technologique. Il est nécessaire de procéder progressivement et par étapes, en testant différentes parties de l'EC. Ce morcellement permet à l'équipe de gestion des risques de focaliser son action sur le dernier sous-ensemble de recommandations prioritaires et ayant le plus d'effet de réduction. Par la suite, l'équipe de tests d'intrusion changera la portée des tests en privilégiant une autre partie de l'environnement numérique de l'entreprise. Ce changement sera conditionné par le processus

d'amélioration continue qui visera à diversifier les tests effectués en ciblant d'autres types d'actifs sensibles et n'ayant pas été testés auparavant.

De plus, pour continuer dans la lignée des limitations, il est important de citer le biais d'évaluation que pourrait entrainer cette quantification des risques. En effet, ITREM repose en partie sur un moteur de calcul quantitatif et pondéré. Il pourrait s'avérer que les sommes pondérées, dans certains cas spéciaux, engendrent une aberration en termes d'évaluation quantitative. Cependant, nous pouvons pallier en partie ce genre d'aberration de calcul en prodiguant des comparatifs et vérifications avec les résultats cumulés de toutes les missions de tests d'intrusions (BDOV).

Il est envisageable d'optimiser les dépenses en termes de sécurité en songeant à une impartition de ces données et actifs numériques vers des fournisseurs d'infonuagique qui assureront eux-mêmes la sécurité des données corporatives. Mais n'est-ce pas là d'autres types de considération de risque et de postures de sécurité à prendre en compte, sachant que les infrastructures où reposent les données n'appartiennent plus au propriétaire légitime de ces dernières ?

De façon à pouvoir faire évoluer cette méthodologie, il sera nécessaire de se concentrer sur deux aspects technologiques majeurs. Le premier sera la création d'une plateforme applicative permettant de pouvoir représenter la logique de la méthodologie et de l'intégrer dans des entreprises sans avoir besoin d'un expert. Cela permettrait d'en faire réellement un outil de référence contenant un registre des risques identifiés et évalués, des indicateurs de posture de sécurité, des comparatifs d'années en années ainsi que d'autres fonctionnalités.

De plus, comme cité précédemment, la tendance actuelle en termes d'impartition de données permet de constater un engouement pour les plateformes de type infonuagique. Ces dernières permettent de favoriser la flexibilité et l'accessibilité de l'accès aux données. Le second point d'intérêt pour faire évoluer notre méthodologie sera la mise en place de listes de contrôles spécifiques aux environnements infonuagiques. Ces listes traiteront des problématiques légales, technologiques, infrastructurelles, et de sécurité. Elles permettront d'évaluer la posture de risque des données en fonction du fournisseur, de ses mesures de protection, ainsi que de ses clauses contractuelles.

La création de cette méthodologie permet de repenser une partie d'un système de gestion des risques dans le domaine extrêmement vaste de la gestion des informations. Nous sommes dans une ère où la détermination de la criticité des actifs est nécessaire et va de pair avec une protection adaptée. Ce portrait utopique de la protection optimale de l'information ne pourra jamais être entièrement dressé, car les environnements numériques évoluent et changent très vite. La gouvernance, la cohésion et la réactivité des équipes de sécurité peuvent être améliorées et tendre vers des critères de maturités plus élevés en ce qui a trait à leurs pratiques et contrôles de sécurité.

Une réflexion postérieure, relative à l'intelligence artificielle, orienterait les futurs travaux vers la création d'un logiciel automatisé permettant d'effectuer les tests d'intrusions, d'analyser les vulnérabilités selon les critères du segment d'affaires de la criticité des données, de les classer selon les EV, et de produire les plans de traitement.

LISTE DE RÉFÉRENCES

[1] Agence nationale de la sécurité des systèmes d'information (ANSSI), «Guides de bonnes pratiques,» [En ligne]. Available: http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/.

[2] International Organization for Standardizaton, «ISO 31000:2009 - Risk management -- Principles and guidelines,» 2009. [En ligne]. Available: http://www.iso.org/.

[3] R. Baloch, Ethical Hacking and Penetration Testing Guide, Boca Raton: CRC Press, 2014.

[4] A. Jones, Risk management for computer security: protecting your network and information assets, Amsterdam: Elsevier Butterworth Heinemann, 2005.

[5] Tenable, [En ligne]. Available: www.tenable.com.

[6] A. Fielder et C. Hankin, Decision support approaches for cyber security investment, London: Elsevier, 2016.

[7] «Penetration Testing Execution Standard (PTES),» [En ligne]. Available: www.pentest-standard.org.

[8] D. Maynor, Metasploit toolkit for penetration testing, Burlington: Syngress, 2007.

[9] Open Web Application Security Project (OWASP), [En ligne]. Available: http://www.owasp.org.

[10] Cyberworld Awareness and Security Enhancement Services, «CASES,» [En ligne]. Available: http://www.cases.lu.

[11] CIGREF : Réseau de grandes entreprises, [En ligne]. Available: http://www.cigref.fr.

[12] The Congress of the United States of America, «Public Law 107 - 296 - Homeland Security Act of 2002,» Washington, 2002.

[13] M. Philips, «Using a Capability Maturity Model to Derive Security Requirements,» 13 March 2003. [En ligne]. Available: https://www.sans.org/reading-room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements-1005.

[14] ISACA, [En ligne]. Available: www.isaca.org.

[15] R. Oppliger, «Quantitative risk analysis in information security management: a modern fairy tale,» *IEEE Security Privacy,* vol. 13 , pp. pp. 18-21, 2015.

[16] Alien Vault, *Open Threat Exchange,* San Mateo.

[17] P. Mell, K. Scarfone et S. Romanosky, «A Complete Guide to the Common Vulnerability Scoring System Version 2.0,» 2007. [En ligne]. Available: https://www.first.org/cvss/v2/guide. [Accès le 2014].

[18] J. Leplat, Apprentissage organisationnel. Théorie, méthode, pratique de Argyris et Schön, Paris: DeBoeck Université, 2002.

[19] M. Leitch, ISO 31000:2009—The New International Standard on Risk Management, London: Blackwell Publishing, 2010.

[20] International Organization for Standardization, «ISO/IEC 27002:2013 - Information technology -- Security techniques,» 2013. [En ligne]. Available: https://www.iso.org/standard/54533.html.

[21] Center for Internet Security, «CIS Benchmarks,» [En ligne]. Available: http://benchmarks.cisecurity.org/downloads/.

[22] International Organization for Standardization, «ISO/IEC 27001 Information security management,» 2013. [En ligne]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[23] A. Calder, The Case for ISO 27001 (2013) Second Edition, London: IT Governance Ltd, 2013.

[24] S. Fenz et E. Weippl, «Ontology based IT-security planning,» chez *12th Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2006.

[25] X. Chen et Y. Li, «Network Security Evaluation Based on Support Vector Machine,» chez *2nd International Conference on Green Communications and Networks 2012 (GCN 2012)*, 2013.

[26] V. Vapnik, Support-Vector Networks, Kluwer Academic Publisher, 1995.

[27] V. Vapnik, Estimation of Dependences Based on Empirical Data, Washington: Springer, 2006.

[28] B. Boser, I. Guyon et V. Vapnik, «A training algorithm for optimal margin classifiers,» chez *5th Annual Workshop on Computational Learning Theory (COLT'92)*, 1992.

[29] C.-C. C. a. .-J. Lin, *LIBSVM,* Taipei: National Taiwan University, December 14, 2015;.

[30] L. Buitinck, G. Louppe, M. Blondel, F. Pedregosa, A. Muller, O. Grisel, V. Niculae, P. Prettenhofer, A. Gramfort, J. Grobler, R. Layton, J. Vanderplas, A. Joly, B. Holt et G. Varoquaux, «{API} design for machine learning software: experiences from the scikit-learn,» chez *European Conference on Machine Learning and Principles and Practices of Knowledge Discovery in Databases*, 2013.

[31] P. Herzog, «Open Source Security Testing Methodology Manual (OSSTMM),» ISECOM, [En ligne]. Available: http://www.isecom.org/research/. [Accès le 2015].

[32] Open Web Application Security Project (OWASP), «Attack,» [En ligne]. Available: https://www.owasp.org/index.php/Category:Attack.

[33] National Institute of Science and Technology, «SP 800-30,» NIST Information Quality Standards, Gaithersburg, September 2012.

[34] National Institute of Standard and Technology (NIST), «FIPS PUB 199: Standards for Security Categorization of Federal Information Systems,» [En ligne]. Available: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

ANNEXE A — BASE DE DONNÉES DE TESTS

NET-VULNDISC	**Vulnerability discovery**
NET-VULNDISC-001	**Passive**
NET-VULNDISC-001.1	Traffic monitoring
NET-VULNDISC-001.2	Metadata analysis
NET-VULNDISC-002	**Active**
NET-VULNDISC-002.1	Automated testing
NET-VULNDISC-002.2	Network vulnerability scanners
NET-VULNDISC-002.2.1	Port based
NET-VULNDISC-002.2.2	Service based
NET-VULNDISC-002.3	Protocol fuzzing
NET-VULNDISC-003	**Research**
NET-VULNDISC-003.1	Public research
NET-VULNDISC-003.1.1	Vulnerability Databases
NET-VULNDISC-003.1.2	Vender advisories
NET-VULNDISC-003.1.3	Exploitation framework
NET-VULNDISC-003.1.4	Common and default password

ANNEXE B — RÉFÉRENCE À UN TEST

Web and Application Intrusion Testing			
Configuration and	CONFIG-002	Test name	Test Application Platform Configuration
		Test details	Proper configuration of the single elements that make up an application architecture is important in order to prevent mistakes that might compromise the security of the whole architecture. Configuration review and testing is a critical task in creating and maintaining an architecture. This is because many different systems will be usually provided with generic configurations that might not be suited to the task they will perform on the specific site they're installed on. While the typical web and application server installation will contain a lot of functionality (like application examples, documentation, test pages) what is not essential should be removed before deployment to avoid post-install exploitation.

ANNEXE C — CATÉGORIES D'ENSEMBLE DE VULNÉRABILITÉS

Réf.	Catégorie de contrôle	Objectifs
5.1	**Orientations de la direction en matière de sécurité de l'information**	Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.
6.1	**Organisation interne**	Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation.
6.2	**Appareils mobiles et télétravail**	Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.
8.1	**Responsabilités relatives aux actifs**	Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée.
8.2	**Classification de l'information**	S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.
8.3	**Manipulation des supports**	Empêcher la divulgation, la modification, le retrait ou la destruction non autorisés de l'information de l'organisation stockée sur des supports.
9.1	**Exigences métier en matière de contrôle d'accès**	Limiter l'accès à l'information et aux moyens de traitement de l'information.

9.2	**Gestion de l'accès utilisateur**	Maitriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non-autorisés aux systèmes et services d'information.
9.3	**Responsabilités des utilisateurs**	Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.
9.4	**Contrôle de l'accès au système et à l'information**	Empêcher les accès non-autorisés aux systèmes et aux applications.
10.1	**Mesures cryptographiques**	Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.
11.1	**Zones sécurisées**	Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.
11.2	**Matériels**	Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.
12.1	**Procédures et responsabilités liées à l'exploitation**	Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.
12.2	**Protection contre les logiciels malveillants**	S'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.
12.3	**Sauvegarde**	Se protéger de la perte de données.
12.4	**Journalisation et surveillance**	Enregistrer les évènements et générer des preuves.
12.5	**Maitrise des logiciels en exploitation**	Garantir l'intégrité des systèmes en exploitation.

12.6	**Gestion des vulnérabilités techniques**	Empêcher toute exploitation des vulnérabilités techniques.
12.7	**Considérations sur l'audit des systèmes d'information**	Réduire au minimum l'impact des activités d'audit sur les systèmes en exploitation.
13.1	**Gestion de la sécurité des réseaux**	Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.
13.2	**Transfert de l'information**	Maintenir la sécurité de l'information transférée au sein de l'organisme et vers une entité extérieure.
14.1	**Exigences de sécurité applicables aux systèmes d'information**	Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d'information fournissant des services sur les réseaux publics.
14.2	**Sécurité des processus de développement et d'assistance technique**	S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.
14.3	**Données de test**	Garantir la protection des données utilisées pour les tests.
15.1	**Sécurité dans les relations avec les fournisseurs**	Garantir la protection des actifs de l'organisation accessible aux fournisseurs.
15.2	**Gestion de la prestation du service**	Maintenir le niveau convenu de sécurité de l'information et de service conforme aux accords conclus avec les fournisseurs.
16.1	**Gestion des incidents liés à la sécurité de l'information et améliorations**	Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des évènements et des failles liés à la sécurité.

17.1	**Continuité de la sécurité de l'information**	La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité.
17.2	**Redondances**	Garantir la disponibilité des moyens de traitement de l'information.
18.1	**Conformité aux obligations légales et règlementaires**	Éviter toute violation des obligations légales, statutaires, règlementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.
18.2	**Revue de la sécurité de l'information**	Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

ANNEXE D — TABLEAU DE CLASSIFICATION DES VULNÉRABILITÉS ET RISQUES ASSOCIÉS

ID	Name	Ensemble de vulnérabilité	Potentialité	Impact	Risque A/CA	Risque A/CR
T1	**Escalade de privilège à partir d'un poste de travail d'un employé typique**					
T1.1	Divulgation d'information de type GPP pour les mots de passe administratifs	EV 1	Modérée	Élevé	Modéré	Faible
T1.2	Protocoles activés (LLMNR & NBTNS)	EV 1	Modérée	Modéré	Modéré	Faible
T1.3	Signature SMB non obligatoire	EV 1	Modérée	Modéré	Modéré	Faible
T1.4	Mots de passe faibles	EV 2	Modérée	Modéré	Modéré	Faible

T1.5	Les paramètres de proxy par défaut n'utilisant pas WPAD	EV 1	Modérée	Imperceptible	Imperceptible	Imperceptible
T2	**Chiffrement du poste de travail**					
T2.1	Attaque DMA	EV 3	Modérée	Élevé	Modéré	Modéré
T3	**Test Wi-Fi**					
T3.1	Absence d'isolation entre les utilisateurs sur le réseau Wi-Fi invité.	EV 1	Modérée	Modéré	Modéré	Imperceptible
T3.2	Détournement de session utilisateur sur FINTRADE visiteur	EV 7	Modérée	Modéré	Modéré	Imperceptible
T3.3	Absence de filtrage entre les VLAN.	EV 7	Modérée	Modéré	Modéré	Faible
T4	**Test d'ingénierie sociale**					
T4.1	Dispersion de clés USB	EV 4	Modérée	Modéré	Modéré	Modéré
T5	**Test de sécurité physique**					

T5.1	Talonnage en zone restreinte	EV 4	Modérée	Modéré	Modéré	Modéré
T6	**Sécurité du processus de virtualisation**					
T6.1	Certaines données sont transférées entre la pré-production et la production	EV 6	Modérée	Modéré	Modéré	Faible
T6.2	Compte d'ancien utilisateur non démissionné	EV 5	Modérée	Modéré	Modéré	Faible
T7	**Sécurité du processus de sauvegarde**					
T7.1	Les données sont accessibles sur le site du fournisseur de solution	EV 3	Modérée	Modéré	Modéré	Faible
T7.2	Les sauvegardes ne peuvent pas être rétablies à temps (RTO)	EV 8	Modérée	Modéré	Modéré	Faible
T8	**Tests de sécurité réseau**					

T8.1	Version non prise en charge de Windows Server 2003	EV 6	Modérée	Élevé	Élevé	Faible
T8.2	Multiples vulnérabilités dans HP System Management Homepage	EV 6	Modérée	Élevé	Modéré	Faible
T8.3	Vulnérabilités relatives aux configurations SSL/TLS	EV 3	Modérée	Modéré	Modéré	Faible
T8.4	La signature SMB est désactivée	EV 1	Modérée	Modéré	Modéré	Imperceptible
T8.5	MITM sur Microsoft Windows Remote Desktop Protocol/Terminal Services	EV 1	Modérée	Modéré	Modéré	Modéré
T8.6	Authentification SMB de type session NULL	EV 1	Modérée	Modéré	Modéré	Imperceptible
T8.7	SSLv3 (POODLE)	EV 3	Modérée	Modéré	Modéré	Imperceptible
T8.8	Multiples vulnérabilités relatives à la configuration SSH	EV 3	Modérée	Faible	Faible	Imperceptible

ANNEXE E — EFFET DES CONTRÔLES SUR LE TRAITEMENT

Référentiel ISO/IEC 27002	Contrôles	Effet des contrôles				
		Dissuasif	Écartement	Préventif	Détection	Réactif
5	**1**					
5.1	**Politique de sécurité de l'information**					
5.1.1	Politique de sécurité de l'information - Document	✓	✓	✓		✓
5.1.2	Revue de la politique de sécurité de l'information	✓	✓	✓		✓
6	**Organisation de la sécurité de l'information**					
6.1	**Organisation interne**					
6.1.1	Engagement de la direction	✓	✓	✓		✓
6.1.2	Coordination de la sécurité		✓	✓		✓
6.1.3	Responsabilités relatives à la sécurité informationelle		✓	✓	✓	✓
6.1.4	Processus d'autorisation pour les centres de données		✓			
6.1.5	Entente de confidentialité		✓	✓		
6.1.6	Contact avec les autorités		✓			✓
6.1.7	Contact avec des groupes d'intérets communs		✓	✓	✓	
6.1.8	Revue indépendant de la sécurité de l'information		✓	✓	✓	✓